*Department of Computer & Information Science*

*Technical Reports (CIS)*

*University of Pennsylvania* *Year* 2008

# A Default Temporal Logic for Regulatory Conformance Checking

Nikhil Dinesh* Aravind K. Joshi†

Insup Lee‡ Oleg Sokolsky**

*University of Pennsylvania, nikhild@seas.upenn.edu

†University of Pennsylvania, joshi@cis.upenn.edu

‡University of Pennsylvania, lee@cis.upenn.edu

**University of Pennsylvania, sokolsky@cis.upenn.edu

University of Pennsylvania Department of Computer and Information Science Technical Report No. MS-CIS-08-07.

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **2008** | | **00-00-2008 to 00-00-2008** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **A Default Temporal Logic for Regulatory Conformance Checking** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **University of Pennsylvania,Department of Computer Science,Philadelphia,PA,19104** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT
**see report**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | **Same as Report (SAR)** | **29** | |

# A Default Temporal Logic for Regulatory Conformance Checking*

Nikhil Dinesh, Aravind Joshi, Insup Lee, and Oleg Sokolsky

Department of Computer Science
University of Pennsylvania
Philadelphia, PA 19104-6389, USA
{nikhild,joshi,lee,sokolsky}@seas.upenn.edu

**Abstract.** This paper considers the problem of checking whether an organization conforms to a body of regulation. Conformance is cast as a trace checking question – the regulation is represented in a logic that is evaluated against an abstract trace or run representing the operations of an organization. We focus on a problem in designing a logic to represent regulation.
A common phenomenon in regulatory texts is for sentences to refer to others for conditions or exceptions. We motivate the need for a formal representation of regulation to accomodate such references between statements. We then extend linear temporal logic to allow statements to refer to others. The semantics of the resulting logic is defined via a combination of techniques from Reiter's default logic and Kripke's theory of truth.
This paper is an expanded version of [1].

## 1 Introduction

Regulations, laws, and policies that affect many aspects of our lives are represented predominantly as documents in natural language. For example, the Food and Drug Administration's Code of Federal Regulations [2] (FDA CFR) governs the operations of American bloodbanks. The CFR is framed by experts in the field of medicine, and regulates the tests that need to be performed on donations of blood before they are used. In such safety-critical scenarios, it is desirable to assess formally whether an organization (bloodbank) conforms to the regulation (CFR).

There is a growing interest in using formal methods to assist organizations in complying with regulation [3–5]. Assisting an organization in compliance involves a number of tasks related to the notion of a violation. For example, it is of interest to detect or prevent violations, assign blame, and if possible, recover from violations. In this paper, we focus on *conformance checking* which involves detecting the presence of violations.

We cast conformance checking as a trace-checking question. The regulation is translated to statements in a logic which are evaluated against a trace or run representing the operations of an organization. The result of evaluation is either an affirmative answer to conformance, or a counterexample representing a subset of the operations of the organization and the specific law that is violated.

* This research was supported in part by NSF CCF-0429948, NSF-CNS-0610297, ARO W911NF-05-1-0158, and ONR MURI N00014-07-1-0907.

There are two important features of regulatory texts that need to be accomodated by a representation in logic. First, regulations convey constraints on an organization's operations, and these constraints can be obligatory (required) or permitted (optional). Second, statements in regulation refer to others for conditions or exceptions. An organization conforms to a body of regulation iff it satisfies all the obligations. However, permissions provide exceptions to obligations, indirectly affecting conformance. Our formulation of obligations and permissions follows the theory of Ross [6], and we will discuss the relationship to other theories (cf. [7]) in Section 3.1.

The central focus of this work is the function of regulatory sentences as conditions or exceptions to others. This function of sentences makes them dependent on others for their interpretation, and makes the translation to logic difficult. We call this the problem of *references to other laws*. In Section 2, we argue that a logic to represent regulation should provide mechanisms for statements to refer to others. We provide motivation using examples from the FDA CFR. We discuss how these sentences can be represented in a logic without references, and conclude that this would make the translation difficult.

We then turn to the task of defining a logic that lets statements refer to and reason about others. In Section 3.1, we define a trace or run-based representation for the operations of an organization, and a predicate-based linear temporal logic (PredLTL) to make assertions about runs. PredLTL is extended to express two kinds of normative statements (obligations and permissions), leading to a formal definition of conformance.

In Sections 3.2 and 3.3, we extend PredLTL to allow references between laws thereby making permissions relevant to conformance. Specifically, we introduce *an inference predicate*, whose interpretation is determined by inferences from laws. The justifications in default logic [8] can be cast as an instance of this predicate. Default logic has been used in computing extensions to a theory, in the manner of logic programs [9, 10]. In conformance checking, we need to separate two uses of statements: (a) extending a theory (the regulation), and (b) determining facts about an organization. This separation is achieved using the inference predicate. Statements are evaluated using the fixed points of an appropriate function, based on a technique used in Kripke's theory of truth [11].

An axiomatization is discussed in Section 4. And, Section 5 concludes with a discussion of related and future work.

## 2 Motivation

In this section, we argue that a logic to represent regulation should provide a mechanism for sentences to refer to others. We discuss shortened versions of sentences from the CFR Section 610.40, which we will use as a running example throughout the paper. Consider the following sentences:

(1) Except as specified in (2), every donation of blood or blood component must be tested for evidence of infection due to Hepatitis B.

(2) You are not required to test donations of source plasma for evidence of infection due to Hepatitis B.

Statement (1) conveys an obligation to test donations of blood or blood component for Hepatitis B, and (2) conveys a permission not to test a donation of source plasma (a blood component) for Hepatitis B. To assess an organization's conformance to (1) and (2), it suffices to check whether "All non-source plasma donations are tested for Hepatitis B". In other words, (1) and (2) imply the following obligation:

(3) Every non-source plasma donation must be tested for evidence of infection due to Hepatitis B.

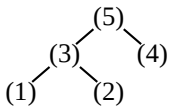
There are a variety of logics in which one can capture the interpretation of (3), as needed for conformance. Now suppose we have a sentence that refers to (1):

(4) To test for Hepatitis B, you must use a screening test kit.

The reference is more indirect here, but the interpretation is: "If (1) requires a test, then the test must be performed using a screening test kit". A bloodbank is not prevented from using a different kind of test for source plasma donations. (4) can be represented by first producing (3), and then inferring that (3) and (4) imply the following:

(5) Every non-source plasma donation must be tested for evidence of infection due to Hepatitis B using a screening test kit.

It is easy to represent the interpretation of (5) directly in a logic. However, (5) has a complex relationship to the sentences from which it was derived, i.e., (1), (2) and (4). The derivation takes the form of a tree:




To summarize, if one wishes to use a logic with no support for referring to other sentences, derived obligations must be created manually. We argue that the manual creation of derived obligations is impractical in terms of the amount of effort involved. We give two (pragmatic) reasons. First, the derived obligation can become very complex. The full version of statement (1) in the CFR contains six exceptions, and these exceptions in turn have statements that qualify them further. It is difficult to inspect a derived obligation, and determine if it captures the intended interpretation of the sentences from which it came. Second, references between laws are frequent, amplifying the effort in creating a logic representation. In [12], we discuss lexical statistics which suggest that references are a common way of establishing relationships between sentences in the CFR, and [13, 4] point out their frequency in other bodies of regulation.

We advocate an approach that allows us to introduce references into the syntax of the logic, and resolve references during evaluation.

## 3 Representing Regulatory Documents in Logic

In this section, we extend linear temporal logic (LTL) to distinguish between obligations and permissions, and allow references between statements. We begin, in Section 3.1, by

representing a bloodbank as a run or trace. LTL is extended to distinguish between obligations and permissions, leading to definitions of conformance. We then extend the logic to allow sentences to refer to others. Section 3.2 gives an informal example-driven account, and Section 3.3 provides a formal account. The complexity of conformance checking is examined in Section 3.4

Sections 3.1 is intended as background, in which we discuss several underlying assumptions. Our goal is to focus on the problem of references, and to treat the representation of obligations and permissions as an important but orthogonal issue.

### 3.1 Predicate-based Linear Temporal Logic (PredLTL)

**Representing regulated operations:** Given the need to demonstrate conformance to the regulation in case of an audit, regulated organizations such as bloodbanks keep track of their operations in a database, for example, donor information and the tests they perform. Such a system can be thought of abstractly as a relational structure evolving over time. At each point in time (state), there are a set of objects (such as donations and donors) and relations between the objects (such as an association between a donor and her donations). The state changes by the creation, removal or modification of objects. We represent this as a run.

**Definition 1 (A Run of a System).** *Given a set $O$ (of objects) and countable sets $\Phi_1, ..., \Phi_n$ (where $\Phi_j$ is a set of predicate names of arity $j$), a run of a system $R(O, \Phi_1, ..., \Phi_n)$, abbreviated as $R$, is a tuple $(r, \pi_1, ..., \pi_n)$ where:*

- *$r : N \rightarrow S$ is a sequence of states. $N$ is the set of natural numbers, and $S$ is a set of states.*
- *$\pi_j : \Phi_j \times S \rightarrow 2^{O^j}$ is a truth assignment to predicates of arity $j$. Given $p \in \Phi_j$, we will say that $p(o_1, ..., o_j)$ is true at state $s$ iff $(o_1, ..., o_j) \in \pi_j(p, s)$.*

Given a run $R$ and a time $i \in N$, the pair $(R, i)$ is called a point (statements in linear temporal logic are evaluated at points). Given the predicate names $(\Phi_1, ..., \Phi_n)$, the corresponding space of runs is denoted by $\mathcal{R}(\Phi_1, ..., \Phi_n)$, abbreviated as $\mathcal{R}$.

Conceivably, we could construct a state-transition diagram representing all possible behaviors of the system and explore conformance from the model checking perspective (e.g., [14]). We chose to restrict our attention to traces for two reasons. First, checking of traces is easier to explain, and all interesting theoretical and algorithmic aspects that we explore in this paper manifest themselves in trace checking. Second, many parts of the operations of an organization, such as a bloodbank, do not involve computers. A complete model of operations has to include a model of human users, which is a research problem in its own right that is well beyond the scope of this paper. However, if a finite-state model of an organization can be created, the propositional version of the logic developed here can be adapted to work with available model-checkers.

**Representing the regulation:** The logic that we define in this section is a restricted fragment of first-order modal logic. The restriction is that we allow formulas with free variables, but no quantification over objects. Formulas will be interpreted using the universal generalization rule, i.e., over all assignments to free variables. The restrictions

are similar in spirit to the logic programing approaches to regulation [9, 10]. PredLTL is less expressive than the variants of first-order logic used by [3, 5]. However, when references are added, the logic becomes more expressive than first-order logic (Section 3.4).

**Definition 2 (Syntax).** *Given sets $\Phi_1, ..., \Phi_n$ (of predicate names) and a set of variables $X$, the language $L(\Phi_1, ..., \Phi_n, X)$, abbreviated as $L$, is the smallest set such that:*

- $p(y_1, ..., y_j) \in L$ *where* $p \in \Phi_j$ *and* $(y_1, ..., y_j) \in X^j$.
- *If* $\varphi \in L$, *then* $\neg\varphi \in L$ *and* $\Box\varphi \in L$. *If* $\varphi, \psi \in L$, *then* $\varphi \wedge \psi \in L$.

Disjunction $\varphi \vee \psi = \neg(\neg\varphi \wedge \neg\psi)$ and implication $\varphi \Rightarrow \psi = \neg\varphi \vee \psi$ are derived connectives. The temporal operator is understood in the usual way: $\Box\varphi$ ($\varphi$ holds and will always hold (globally)). $\Diamond\varphi$ ($\varphi$ will eventually hold) is defined as $\neg\Box\neg\varphi$.

We now extend the syntax to express normative statements in a body of regulation, by distinguishing between obligations and permissions.

**Definition 3 (Syntax of Regulation).** *Given a finite set of identifiers $ID$, a body of regulation $Reg$ is a set of statements such that for each $id \in ID$, there exist $\varphi, \psi \in L$ such that either: $id$.***o***: $\varphi \rightsquigarrow \psi \in Reg$, or $id$.***p***: $\varphi \rightsquigarrow \psi \in Reg$*

id.**o**: $\varphi \rightsquigarrow \psi$ (id.**p**: $\varphi \rightsquigarrow \psi$) is read as: "it is obligated (permitted) that the precondition $\varphi$ leads to the postcondition $\psi$". The distinction between preconditions and postconditions corresponds to the distinction between input and output in input-output logic [15].

**Definition 4 (Semantics).** *Given a run $R = (r, \pi_1, ..., \pi_n)$, $i \in N$, $\varphi \in L$, and an assignment $v : X \to O$, the relation $(R, i, v) \models \varphi$ is defined inductively as follows:*

- $(R, i, v) \models p(y_1, ..., y_j)$ *iff* $(o_1, ..., o_j) \in \pi_j(p, r(i))$ *where* $o_k = v(y_k)$ *if* $y_k \in O$.
- *The semantics of conjunction and negation is defined in the usual way.*
- $(R, i, v) \models \Box\varphi$ *iff for all* $k \geq i : (R, k, v) \models \varphi$

*We extend the semantic relation to regulatory statements. We take $\models$ to stand for "conforms to":*

- $(R, i, v) \models$ *id.***o***: $\varphi \rightsquigarrow \psi$ iff* $(R, i, v) \models \varphi \Rightarrow \psi$ *($\Rightarrow$ is implication)*
- $(R, i, v) \models$ *id.***p***: $\varphi \rightsquigarrow \psi$. Runs vacuously conform to permissions. Permissions will become relevant when references from obligations are present (Section 3.2).*

Consider again our example from Section 2. We use three predicates defined as follows. $d(x)$ is true iff $x$ is a donation. $sp(x)$ is true iff $x$ consists of source plama. $test(x)$ is true iff $x$ is tested for Hepatitis B. Statement (3) is represented as:

3.**o**: $d(x) \wedge \neg sp(x) \rightsquigarrow \Diamond test(x)$

Statement (2) is be represented as: 2.**p**: $d(y) \wedge sp(y) \rightsquigarrow \neg\Diamond test(y)$. However, statement (1) cannot be represented directly.

We will now define conformance, and then discuss the various definitions in the context of related work. Given a run $R$, let $V(R)$ denote the set of variable assignments. Conformance is defined using the notion of validity. A formula $\varphi$ is valid at the point $(R, i)$, denoted $(R, i) \models \varphi$, iff for all $v \in V(R)$: $(R, i, v) \models \varphi$. A formula $\varphi$ is valid on $R$ iff it is valid at all points, that is, $R \models \varphi$ iff for all $i \in N : (R, i) \models \varphi$.

**Definition 5 (Run Conformance).** *Given a body of regulation $Reg$ and a run $R$ representing the operations of an organization, we say that $R$ conforms to the regulation iff for all obligations $id$.***o***: $\varphi \rightsquigarrow \psi \in Reg$, we have $R \models id$.***o***: $\varphi \rightsquigarrow \psi$.*

**Discussion:** The deontic concepts of obligation and permission are treated as properties of sentences. Only obligations matter for conformance. If a non-source plasma donation is not tested, there is a problem. On the other hand, a bloodbank may choose to test a donation of source plasma or not. In assessing conformance, the function of a permission is to serve as an exception to an obligation, and in this indirect manner it becomes relevant. We will give a semantics to this function of permissions in Section 3.2. Such a treatment of permissions has its basis in the legal theory of Ross [6].

Ross' approach to permission is by no means the only one. Theories have distinguished between various kinds of permission (cf. [7]), the most common distinction being that of positive and negative permission. We discuss the analysis by Makinson and van der Torre [16]. $\varphi$ is said to positively permitted iff it is explictly permitted by the laws, and $\varphi$ is negatively permitted iff it is not forbidden. The key issue is whether positive permissions can give rise to violations. In regulations phrased exclusively in terms of permissions, it is desirable to say that *if $\varphi$ denotes a "relevant" condition which is not explicitly permitted, then it should not hold in conforming implementations*. While this has been analysed as a property of permission, following Ross, we take such violations as arising from an implicit obligation, i.e., the italicized clause. This implicit obligation can be represented using the techniques we discuss in Section 3.2, provided that the relevance of the condition is known.

In the formulation here, obligations and permissions are top-level operators and cannot be negated. This restriction can be removed by treating obligation and permission as KD modalities (c.f. [17]), and using a many-valued interpretation to decide if a run belongs to the set of ideal runs. However, we avoid this to simplify presentation. A more crucial restriction is that iterated deontic constructs cannot be expressed directly, i.e., sentences of the form "required to allow x" or "allowed to require x.". One has to decide what top-level obligations or permissions are implied by these constructs. To our knowledge, handling iterated constructs is an open problem in deontic logic [18].

### 3.2 References to Other Laws – An Informal Description

In this section, we give an informal account of *reference logic* (RefL), which is used to handle references. We extend the syntax of PredLTL with *an inference predicate* $\mathrm{by}_{\mathrm{Id}}(\varphi)$, where Id is a set of identifiers. $\mathrm{by}_{\mathrm{Id}}(\varphi)$ is read as "by the laws in Id, $\varphi$ holds". There are two restrictions: (a) $\varphi$ is a statement in PredLTL (Definition 2) and (b) the predicate $\mathrm{by}_{\mathrm{Id}}(\varphi)$ can appear only in preconditions of laws. These restrictions are similar to those that apply to justifications in default logic [8].

Consider again our example statements (1) and (2), which are represented in RefL as follows:

- 1.**o**: $d(x) \wedge \neg \mathrm{by}_{\{2\}}(\varphi(x)) \rightsquigarrow \Diamond test(x)$, and
- 2.**p**: $d(y) \wedge sp(y) \rightsquigarrow \neg \Diamond test(y)$

In the obligation above, the subformula $\mathrm{by}_{\{2\}}(\varphi(x))$ is understood as "by the law (2) the formula $\varphi(x)$ holds". It remains to define the formula $\varphi(x)$. Intuitively, this should be the negation of the postcondition of (1). In other words, if $\neg\Diamond test(x)$ follows from (2), then the postcondition of (1) need not hold. This gives us:

1.**o**: $d(x) \wedge \neg \mathrm{by}_{\{2\}}(\neg\Diamond test(x)) \rightsquigarrow \Diamond test(x)$

We interpret the predicate $\mathrm{by}_{\{2\}}(\neg\Diamond test(x))$, by letting formulas have output. In other words, when the precondition of an obligation or permission is true at a point, the point is *annotated* with the postcondition.

| Time | Objects | Predicates | Annotations |
|---|---|---|---|
| 1 | $o_1$ | $d(o_1)$, $sp(o_1)$, $\neg test(o_1)$ | 2: $\neg\Diamond test(o_1)$ |
| 2 | $o_1$ | $d(o_1)$, $sp(o_1)$, $\neg test(o_1)$ | 2: $\neg\Diamond test(o_1)$ |
| | $o_2$ | $d(o_2)$, $\neg sp(o_2)$, $\neg test(o_2)$ | 1: $\Diamond test(o_2)$ |
| 3 | $o_1$ | $d(o_1)$, $sp(o_1)$, $test(o_1)$ | 2: $\neg\Diamond test(o_1)$ |
| | $o_2$ | $d(o_2)$, $\neg sp(o_2)$, $\neg test(o_2)$ | 1: $\Diamond test(o_2)$ |

**Table 1.** A run and its annotations

Table 1 shows a run of a bloodbank augmented with annotations. First, an object $o_1$ is entered into the system. $o_1$ is a donation of source plasma ($d(o_1)$ and $sp(o_1)$ are true). When a donation is added, its test predicate is initially false. Then, an object $o_2$ is added, which is a donation but not of source plasma. In the third step, the object $o_1$ is tested. At this point, unless the run is extended to test $o_2$ as well, it does not conform with the regulation. We now discuss how the annotations are arrived at and used to assess the regulation.

We begin by defining an annotation. Given a run $R$, an assignment $v \in V(R)$, and $\varphi \in L$, $v(\varphi)$ is the formula obtained by replacing all variables $x$ by the unique name for the object $v(x)$. We assume that all variables are free. Note that $v(\varphi)$ is equivalent to a propositional LTL formula, as the variables have been replaced by constant symbols. An annotation, id: $v(\varphi)$, is a propositional LTL formula associated with an identifier.

Given a point $(R, i)$ and an assignment $v \in V(R)$, first we consider the permission 2.**p**: $d(y) \wedge sp(y) \rightsquigarrow \neg\Diamond test(y)$. If $(R, i, v) \models d(y) \wedge sp(y)$, then $(R, i)$ is *annotated* with 2: $v(\neg\Diamond test(y))$. Otherwise, there is no annotation.

Since the precondition of statement (2) is true for the assignment of $y$ to $o_1$, we have the annotation 2: $\neg\Diamond test(o_1)$ at all points. However, since $o_2$ is not a donation of source plasma, there is no correponding annotation.

Now consider the formula $\mathrm{by}_{\{2\}}(\neg\Diamond test(x))$. This is evaluated as follows. We evaluate 2.**p**: $d(y) \wedge sp(y) \rightsquigarrow \neg\Diamond test(y)$ at $(R, i)$ w.r.t. all variable assignments. Let $\psi_2$ be the conjunction of the annotations produced by the formula for (2).

$(R, i, v) \models \mathrm{by}_{\{2\}}(\neg\Diamond test(x))$ iff $\models \psi_2 \Rightarrow v(\neg\Diamond test(x))$

Notice that this requires a validity check in propositional LTL, which can be decided in space polynomial in the size of the formula [19].

Returning to the run in Table 1, the states are annotated with 2: $\neg\Diamond test(o_1)$ and $\models \neg\Diamond test(o_1) \Rightarrow \neg\Diamond test(o_1)$, since $\varphi \Rightarrow \varphi$ is a propositional tautology. So $(R, i, v) \models \mathrm{by}_{\{2\}}(\neg\Diamond test(x))$ when $v(x) = o_1$.

We can evaluate 1.**o**: $d(x) \wedge \neg\mathrm{by}_{\{2\}}(\neg\Diamond test(x)) \rightsquigarrow \Diamond test(x)$ similarly by annotating states with $\Diamond test(x)$ if the precondition holds. In Table 1, this results in an annotation of 1: $\Diamond test(o_2)$ on the appropriate states. If $o_2$ is never tested, the run will be declared non-conforming (by Definition 5), but the annotation will remain. This lets a law which depends on (1) draw the correct inference.

### 3.3 Reference Logic (RefL)

The semantic evaluation outlined in Section 3.2 works only when the references are acyclic, since an order of evaluation needs to be defined. To handle cycles, we adopt a fixed-point technique from Kripke's theory of truth [11]. The idea is to move to a three-valued logic where the third (middle) value stands for *ungrounded*. Initially, all statements are ungrounded and there are no annotations. Using an inflatonary function, we add annotations until a fixed point in reached. In this section, we define this inflationary function and show that it has least and maximal fixed points. We begin by extending the syntax described in Section 3.1:

**Definition 6 (Syntax of Preconditions).** *Given sets $\Phi_1, ..., \Phi_n$ (of predicate names), a set of variables $X$, and a finite set of identifiers $ID$, the language $L'(\Phi_1, ..., \Phi_n, X, ID)$, abbreviated as $L'$, is the smallest set such that:*

- $p(y_1, ..., y_j) \in L'$ *where* $p \in \Phi_j$ *and* $(y_1, ..., y_j) \in X^j$.
- *If* $\varphi \in L'$, *then* $\neg\varphi \in L'$ *and* $\Box\varphi \in L'$. *If* $\varphi, \psi \in L'$, *then* $\varphi \wedge \psi \in L'$
- *If* $Id \subseteq ID$ *and* $\varphi \in L(\Phi_1, ..., \Phi_n, X)$ *(Definition 2), then* $\mathrm{by}_{\mathrm{Id}}(\varphi) \in L'$

The syntax of regulatory statements (Definition 3) is modified so that the preconditions of laws are statements from $L'$. We use $id.\mathbf{x} : \varphi \rightsquigarrow \psi$ to stand for a normative statement (either obligation or permission). We now define an annotation:

**Definition 7 (Annotation).** *Given a run $R$, a set of identifiers $ID$, an assignment $v \in V(R)$, and a body of regulation $Reg$, an annotation is a statement* id: $v(\psi)$ *such that $id \in ID$ and $id.\mathbf{x} : \varphi \rightsquigarrow \psi \in Reg$. The set of annotations is denoted by $A(R, ID, Reg)$, abbreviated $A$.*

**Definition 8 (Annotation Function).** *Given a run $R$, an annotation function $\alpha : N \to 2^A$ assigns a set of annotations to each point. We use $\alpha.Id(i)$ to denote the set of annotations* id: $\psi \in \alpha(i)$ *such that $id \in Id$.*

We will formalize the semantics using the fixed point technique outlined in [11]. Before we turn to the formal definitions, we sketch some of the key ideas involved.

Let us assume as given a run $R$. Statements in $L'$ and $Reg$ are divided into three classes corresponding to true ($\mathbf{T}(i, v)$), false ($\mathbf{F}(i, v)$) and ungrounded ($\mathbf{U}(i, v)$) w.r.t. the time $i \in N$ and assignment $v \in V(R)$. Intuitively, $\mathbf{U}(i, v)$ is the set of statements that are waiting for the evaluation of another statement.

As we discussed in Section 3.2, to determine whether $\mathrm{by}_{\mathrm{Id}}(\varphi) \in \mathbf{T}(i,v)$, we need to check if there is a set of annotations which imply $v(\varphi)$. We construct the annotation function $\alpha$ such that for all assignments $v$, we have id: $v(\psi) \in \alpha(i)$ iff $\varphi \in \mathbf{T}(i,v)$ for some $id.\mathbf{x}: \ \varphi \rightsquigarrow \psi \in Reg$ and $id \in Id$. We will say that $\mathrm{by}_{\mathrm{Id}}(\varphi) \in \mathbf{T}(i,v)$ only if $\alpha.Id(i) \cup \{v(\neg\varphi)\}$ is not satisfiable.

To determine whether $\mathrm{by}_{\mathrm{Id}}(\varphi) \in \mathbf{F}(i,v)$, we need to ensure that there is no ungrounded statement that could make it true. To check this condition, we construct the annotation function $\alpha'$ such that id: $v(\psi) \in \alpha'(i)$ iff $\varphi \in \mathbf{T}(i,v) \cup \mathbf{U}(i,v)$ for some $id.\mathbf{x}: \ \varphi \rightsquigarrow \psi \in Reg$ and $id \in Id$. The condition for falsity w.r.t. $\alpha'$ is simply the negation of the condition for truth w.r.t. $\alpha$. More formally, $\mathrm{by}_{\mathrm{Id}}(\varphi) \in \mathbf{F}(i,v)$ only if $\alpha'.Id(i) \cup \{v(\neg\varphi)\}$ is satisfiable.

When there are circular references, one cannot always evaluate a statement to be true or false. The Nixon-diamond problem (introduced in [8]) is a well-known example. We rephrase it in "legalese":

(6) Except as otherwise specified, Quakers must be pacifists.

(7) Except as otherwise specified, Republicans must not be pacifists.

These statements can be represented in RefL as follows:
6.**o**: $q(x) \wedge \neg\mathrm{by}_{\{6,7\}}(\neg p(x)) \rightsquigarrow p(x)$, and
7.**o**: $r(x) \wedge \neg\mathrm{by}_{\{6,7\}}(p(x)) \rightsquigarrow \neg p(x)$

Suppose we are given a state with an individual $n$ (for Nixon), who is both quaker and republican, i.e., $q(n)$ and $r(n)$ hold. How should we evaluate the statements above? [11] suggests two answers to this question: (A) The statements are neither true or false (they are ungrounded). This corresponds to skeptical reasoning in non-monotonic logic. (B) Exactly one of $\mathrm{by}_{\{6,7\}}(p(n))$ and $\mathrm{by}_{\{6,7\}}(\neg p(n))$ is true, which leads us to conclude $p(n)$ (by (6)) or $\neg p(n)$ (by (7)) resply. This corresponds to credulous reasoning in non-monotonic logic.

In the semantics we give below, different answers correspond to different fixed points. We refer the reader to [11] for examples and discussion of the various possibilities with regard to fixed points. The choice of what to do when there are multiple fixed points depends on the application, and we discuss this issue further at the end of this section.

**Definition 9 (Evaluation).** *Given a run $R$ and a body of regulation $Reg$, an evaluation is a tuple $E = (\mathbf{T}, \mathbf{F}, \mathbf{U})$, where $\mathbf{T}$, $\mathbf{F}$ and $\mathbf{U}$ are functions of the form $N \times V(R) \rightarrow 2^{L^+}$, where $L^+ = Reg \cup L'$. Furthermore, for all $i \in N$ and $v \in V(R)$, we have $\mathbf{T}(i,v) \cap \mathbf{F}(i,v) = \emptyset$ and $\mathbf{U}(i,v) = 2^{L^+} - (\mathbf{T}(i,v) \cup \mathbf{F}(i,v))$.*

*Given an evaluation $E$, $\alpha_E$ is the annotation such that for all $i \in N$ and $id \in ID$, we have id: $v(\psi) \in \alpha_E(i)$ iff $\varphi \in \mathbf{T}(i,v)$, where $id.\mathbf{x}: \ \varphi \rightsquigarrow \psi \in Reg$. Similarly, $\alpha'_E$ is the annotation such that id: $v(\psi) \in \alpha'_E(i)$ iff $\varphi \in \mathbf{T}(i,v) \cup \mathbf{U}(i,v)$.*

**Definition 10 (Consistent Evaluation).** *An evaluation $E$ is consistent iff for all $i \in N$ and $v \in V(R)$, $\mathbf{T}(i,v) = \mathbf{F}(i,v) = \emptyset$, or $\mathbf{T}(i,v)$ and $\mathbf{F}(i,v)$ are sets such that:*

1. $p(x_1, ..., x_j) \in \mathbf{T}(i,v)$ *iff* $(v(x_1), ..., v(x_j)) \in \pi_j(p, r(i))$
   $p(x_1, ..., x_j) \in \mathbf{F}(i,v)$ *iff* $(v(x_1), ..., v(x_j)) \notin \pi_j(p, r(i))$

2. *If* $\phi \in \mathbf{T}(i,v)$ *and* $\psi \in \mathbf{T}(i,v)$*, then* $\phi \wedge \psi \in \mathbf{T}(i,v)$
   *If* $\phi \in \mathbf{F}(i,v)$ *or* $\psi \in \mathbf{F}(i,v)$*, then* $\phi \wedge \psi \in \mathbf{F}(i,v)$
   *and similarly for negation and temporal operators*
3. *If* $\varphi \Rightarrow \psi \in \mathbf{T}(i,v)$*, then id.***o***:* $\varphi \rightsquigarrow \psi \in \mathbf{T}(i,v)$
   *If* $\varphi \Rightarrow \psi \in \mathbf{F}(i,v)$*, then id.***o***:* $\varphi \rightsquigarrow \psi \in \mathbf{F}(i,v)$
   *id.***p***:* $\varphi \rightsquigarrow \psi \in \mathbf{T}(i,v)$*. Runs vacuously conform to permissions.*
4. *If* $\mathrm{by}_{\mathrm{Id}}(\varphi) \in \mathbf{T}(i,v)$*, then* $\alpha_E.Id(i) \cup \{v(\neg\varphi)\}$ *is not satisfiable.*
   *If* $\mathrm{by}_{\mathrm{Id}}(\varphi) \in \mathbf{F}(i,v)$*, then* $\alpha'_E.Id(i) \cup \{v(\neg\varphi)\}$ *is satisfiable.*

*The set of all consistent evaluations for a run* $R$ *and regulation* $Reg$ *is denoted by* $\mathcal{E}(R, Reg)$*, abbreviated* $\mathcal{E}$*.*

Observe that in consistent evaluations, if $\mathrm{by}_{\mathrm{Id}}(\varphi) \in \mathbf{T}(i,v)$, then $\alpha_E.Id(i) \cup \{v(\neg\varphi)\}$ is not satisfiable (Clause 4 in Definition 10). The converse need not be true.

**Definition 11 (Partial Order).** *Given evaluations* $E_1 = (\mathbf{T}_1, \mathbf{F}_1, \mathbf{U}_1)$ *and* $E_2 = (\mathbf{T}_2, \mathbf{F}_2, \mathbf{U}_2, \alpha_2)$*, we say that* $E_1 \leq E_2$ *iff for all* $i \in N$ *and* $v \in V(R)$*,* $\mathbf{T}_1(i,v) \subseteq \mathbf{T}_2(i,v)$ *and* $\mathbf{F}_1(i,v) \subseteq \mathbf{F}_2(i,v)$*.*

*The pair* $(\mathcal{E}, \leq)$*, where* $\mathcal{E}$ *is the set of consistent evaluations is a partially ordered set (poset).*

We now define the inflationary function whose fixed points we will be interested in.

**Definition 12 (Inflationary function).** *Given* $(\mathcal{E}, \leq)$*, the function* $\mathcal{I} : \mathcal{E} \to \mathcal{E}$ *is defined as follows. Given a consistent evaluation* $E_1 = (\mathbf{T}_1, \mathbf{F}_1, \mathbf{U}_1)$*,* $\mathcal{I}(E_1)$ *is the smallest consistent evaluation* $E_2 = (\mathbf{T}_2, \mathbf{F}_2, \mathbf{U}_2)$ *such that* $E_1 \leq E_2$*, for all* $i \in N$ *and* $v \in V(R)$*,* $\mathbf{T}_2(i,v) \neq \emptyset$*,* $\mathbf{F}_2(i,v) \neq \emptyset$*, and* $E_2$ *extends* $E_1$*.*

*We say that* $E_2$ *extends* $E_1$ *iff for all* $i \in N$ *and* $v \in V(R)$*:*
*If* $\alpha_{E_1}(i) \cup \{v(\neg\varphi)\}$ *is not satisfiable, then* $\mathrm{by}_{\mathrm{Id}}(\varphi) \in \mathbf{T}_2(i,v)$
*If* $\alpha'_{E_1}(i) \cup \{v(\neg\varphi)\}$ *is satisfiable, then* $\mathrm{by}_{\mathrm{Id}}(\varphi) \in \mathbf{F}_2(i,v)$

In the rest of the section, we show that $\mathcal{I}$ is well-defined, and has maximal fixed points and a unique least fixed point. We begin by observing an ordering relation between annotations that is useful in subsequent proofs:

**Proposition 1.** *Given consistent evaluations* $E_1$ *and* $E_2$ *such that* $E_1 \leq E_2$*, and a set of identifiers* $Id \subseteq ID$*, for all* $i \in N$*, we have* $\alpha_{E_1}.Id(i) \subseteq \alpha_{E_2}.Id(i)$ *and* $\alpha'_{E_1}.Id(i) \supseteq \alpha'_{E_2}.Id(i)$*.*

The proof follows easily from Definitions 9 and 11. We now show that $\mathcal{I}$ is well-defined:

**Proposition 2.** *Given* $(\mathcal{E}, \leq)$ *and* $E_1 \in \mathcal{E}$*, let* $\mathcal{E}_2 \subseteq \mathcal{E}$ *be the set of consistent evaluations such that* $E_2 \in \mathcal{E}_2$ *iff* $E_1 \leq E_2$*, for all* $i \in N$ *and* $v \in V(R)$*,* $\mathbf{T}_2(i,v) \neq \emptyset$*,* $\mathbf{F}_2(i,v) \neq \emptyset$*, and* $E_2$ *extends* $E_1$*. Then,* $\mathcal{E}_2$ *has a smallest element.*

*Proof.* Given $E_1$, we construct the evaluation $E_2$ such that for all $i \in N$ and $v \in V(R)$:
$\varphi \in \mathbf{T}_2(i,v)$ iff $\varphi \in \mathbf{T}_1(i,v)$ or:

- $\varphi = \mathrm{by}_{\mathrm{Id}}(\phi)$ and $\alpha_{E_1}.Id(i) \cup \{v(\neg\phi)\}$ is not satisfiable.
- $\varphi = \phi \wedge \psi$ and $\phi, \psi \in \mathbf{T}_2(i,v)$. Similarly for propositions, negation and temporal operators

$\mathbf{F}_2(i,v)$ is defined similarly. It is easy to see that $E_1 \leq E_2$, $E_2$ extends $E_1$ and the non-emptiness condition follows from the existence of at least one atomic proposition. We claim that $E_2$ is consistent and that it is the smallest evaluation with the requisite properties.

Suppose $E_2$ is not consistent. Consider the smallest $\varphi$ which violates Definition 10. We obtain a contradiction for each clause in Definition 10. The only non-trivial case is for $\varphi = \mathrm{by}_{\mathrm{Id}}(\phi)$, for which there are two cases.

$\mathrm{by}_{\mathrm{Id}}(\phi) \in \mathbf{T}_2(i,v)$ and $\alpha_{E_2}.Id(i) \cup \{v(\neg\phi)\}$ is satisifiable. By Proposition 1, $\alpha_{E_1}.Id(i) \subseteq \alpha_{E_2}.Id(i)$, and so $\alpha_{E_1}.Id(i) \cup \{v(\neg\phi)\}$ is satisifiable and $\mathrm{by}_{\mathrm{Id}}(\varphi) \notin \mathbf{T}_1(i,v)$ (since $E_1$ is consistent). It follows from the construction that $\mathrm{by}_{\mathrm{Id}}(\varphi) \notin \mathbf{T}_2(i,v)$ giving us a contradiction.

$\mathrm{by}_{\mathrm{Id}}(\phi) \in \mathbf{F}_2(i,v)$ and $\alpha'_{E_2}.Id(i) \cup \{v(\neg\phi)\}$ is not satisifiable. By Proposition 1, $\alpha'_{E_1}.Id(i) \supseteq \alpha'_{E_2}.Id(i)$, and so $\alpha'_{E_1}.Id(i) \cup \{v(\neg\phi)\}$ is not satisifiable and $\mathrm{by}_{\mathrm{Id}}(\varphi) \notin \mathbf{F}_1(i,v)$ (since $E_1$ is consistent). It follows from the construction that $\mathrm{by}_{\mathrm{Id}}(\varphi) \notin \mathbf{F}_2(i,v)$ giving us a contradiction.

We now show that $E_2$ is the smallest element with the requisite properties, i.e., for all $E'_2 \in \mathcal{E}_2$, we have $E_2 \leq E_2$. The proof is similar to that for consistency. Suppose, for the sake of contradiction, there exists $E'_2 \in \mathcal{E}_2$ such that $E'_2 = (\mathbf{T}'_2, \mathbf{F}'_2, \mathbf{U}'_2)$ and $E_2 \not\leq E'_2$. Consider the smallest $\varphi \in L^+$ such that there exists $i \in N$ and $v \in V(R)$, and $\varphi \in \mathbf{T}_2(i,v) - \mathbf{T}'_2(i,v)$ or $\varphi \in \mathbf{F}_2(i,v) - \mathbf{F}'_2(i,v)$. Again, the only non-trivial case is for $\varphi = \mathrm{by}_{\mathrm{Id}}(\phi)$.

Suppose $\mathrm{by}_{\mathrm{Id}}(\phi) \in \mathbf{T}_2(i,v) - \mathbf{T}'_2(i,v)$. Since $E_1 \leq E'_2$, $\mathrm{by}_{\mathrm{Id}}(\phi) \notin \mathbf{T}_1(i,v)$. There are two cases. If $\alpha_{E_1}.Id(i) \cup \{v(\neg\phi)\}$ is not satisfiable, then $\mathrm{by}_{\mathrm{Id}}(\phi) \in \mathbf{T}'_2(i,v)$ (since $E'_2$ extends $E_1$). This gives us a contradiction. If $\alpha_{E_1}.Id(i) \cup \{v(\neg\phi)\}$ is satisfiable, then $\mathrm{by}_{\mathrm{Id}}(\phi) \notin \mathbf{T}'_2(i,v)$ (by construction). Again, we have a contradiction. So, $\mathrm{by}_{\mathrm{Id}}(\phi) \notin \mathbf{T}_2(i,v) - \mathbf{T}'_2(i,v)$. The other cases are similar. □

The existence of fixed points is established using Zorn's lemma, which applies to chain-complete posets. Given the poset $(\mathcal{E}, \leq)$, a set $\mathcal{E}' \subseteq \mathcal{E}$ is called a chain (totally ordered set) iff for all $E_1, E_2 \in \mathcal{E}'$, we have $E_1 \leq E_2$ or $E_2 \leq E_1$. A poset is chain complete iff every chain has a supremum. We now show that $(\mathcal{E}, \leq)$ is a chain-complete poset:

**Proposition 3.** *$(\mathcal{E}, \leq)$ is a chain-complete poset.*

*Proof.* Given a chain $\mathcal{E}' \subseteq \mathcal{E}$, consider the evaluation:
$E_s = (\mathbf{T}_s, \mathbf{F}_s, \mathbf{U}_s)$, where for all $i \in N$, $v \in V(R)$, and $\varphi \in L^+$:

- $\varphi \in \mathbf{T}_s(i,v)$ iff there exists $E = (\mathbf{T}, \mathbf{F}, \mathbf{U}) \in \mathcal{E}'$ such that $\varphi \in \mathbf{T}(i,v)$.
- $\varphi \in \mathbf{F}_s(i,v)$ iff there exists $E = (\mathbf{T}, \mathbf{F}, \mathbf{U}) \in \mathcal{E}'$ such that $\varphi \in \mathbf{F}(i,v)$.

$\mathbf{U}_s(i,v) = 2^{L^+} - (\mathbf{T}_s(i,v) \cup \mathbf{F}_s(i,v))$. It is immediate from the construction that $\forall E \in \mathcal{E}' : E \leq E_s$. It is also easy to see that if $E_s$ is a consistent evaluation, then it is the supremum of $\mathcal{E}'$. Thus, it suffices to show that $E_s$ is consistent, and this can be established by an argument similar to the proof of Proposition 2. □

**Lemma 1 (Zorn (c.f. [20])).** *Every chain complete poset has a maximal element*

The existence of maximal fixed points is immediate from Zorn's lemma and the fact that $\mathcal{I}$ is inflationary, i.e., $E \leq \mathcal{I}(E)$. Let $E^*$ be a maximal element in $\mathcal{E}$, since $E^*$ is maximal and $E^* \leq \mathcal{I}(E^*)$ it follows that $E^* = \mathcal{I}(E^*)$.

To show the existence of a least fixed point, as [11] notes, we will need the observation that $\mathcal{I}$ *is monotonic*, i.e., if $E_1 \leq E_2$ then $\mathcal{I}(E_1) \leq \mathcal{I}(E_2)$. This can be shown by an argument similar to the proof of Proposition 2. With monotonicity, we obtain the following corollary to Zorn's lemma:

**Corollary 1.** *Given $E_1 \in \mathcal{E}$, let $\sigma(E_1)$ be the smallest set such that: (a) $E_1$ in $\mathcal{E}$, (b) if $E \in \sigma(E_1)$ then $\mathcal{I}(E) \in \sigma(E_1)$, and (c) if $C \subseteq \sigma(E_1)$ is a non-empty chain, then $E_{sc} \in \sigma(E_1)$, where $E_{sc}$ is the supremum of $C$ w.r.t. $\mathcal{E}$. Then:*

- *$\sigma(E_1)$ is a chain whose supremum is a fixed point of $\mathcal{I}$*
- *$\sigma(E_1)$ contains a unique fixed point*
- *If $E_1 \leq E_2$, then $E_{s1} \leq E_{s2}$, where $E_{s1}$ and $E_{s2}$ are the suprema of $\sigma(E_1)$ and $\sigma(E_2)$ resply., and*
- *$\mathcal{I}$ has a unique least fixed point.*

*Proof.* The fact that $\sigma(E_1)$ is a chain is used to prove Zorn's lemma, and we refer the reader to [20] for a proof.

Let $\mathcal{E}' = \sigma(E_1)$ and let $E_s$ be the supremum of $\mathcal{E}'$. Since $\mathcal{E}'$ contains its supremum $E_s$, and $\mathcal{I}(E_s) \in \mathcal{E}'$ (by definition), we can conclude that $E_s = \mathcal{I}(E_s)$.

We now claim that $E_s$ is the unique fixed point in $\mathcal{E}'$. Suppose not. Let $E \in \mathcal{E}'$ be a fixed point. Since $E \neq E_s$ and $E_s$ is the supremum, we have $E < E_s$. Consider the set $\mathcal{E}''$ such that for all $E' \in \mathcal{E}'$, $E' \in \mathcal{E}''$ iff $E' \leq E$. But now, $E_1 \in \mathcal{E}''$ and for all $E' \in \mathcal{E}''$, we have $\mathcal{I}(E') \in \mathcal{E}''$ (for if not $E' \leq E$ and $\mathcal{I}(E) < \mathcal{I}(E')$, contradicting the monotonicity of $\mathcal{I}$). Given a chain $C \subseteq \mathcal{E}''$, since for all $E'' \in C$, we have $E'' \leq E$, $sup(C) \leq E$ (by defintion of supremum). Since $\mathcal{E}'' \subset \mathcal{E}'$, we have a contradiction to the minimality of $\mathcal{E}'$. Hence, $E_s$ is the unique fixed point in $\mathcal{E}'$.

Given $E_1 \leq E_2$, let $E_{s1}$ and $E_{s2}$ be the suprema of $\sigma(E_1)$ and $\sigma(E_2)$ resply. We claim that $E_{s1} \leq E_{s2}$. Suppose not. Consider the set $\mathcal{E}'' \subseteq \sigma(E_1)$ such that $E_1' \in \mathcal{E}''$ iff $E_1' \leq E_{s2}$. But now, $E_1 \in \mathcal{E}''$ and for all $E' \in \mathcal{E}''$, we have $\mathcal{I}(E') \in \mathcal{E}''$ (for if not $E_1' \leq E_{s2}$ and $E_{s2} = \mathcal{I}(E_{s2}) < \mathcal{I}(E_1')$, contradicting the monotonicity of $\mathcal{I}$). The presence of suprema is similarly verified, giving us a contradiction to the minimality of $\sigma(E_1)$. Hence $E_{s1} \leq E_{s2}$.

Finally, let $E_0 = (\mathbf{T}_0, \mathbf{F}_0, \mathbf{U}_0)$, where for all $i \in N$, $v \in V(R)$, $\mathbf{T}_0(i, v) = \mathbf{F}_0(i, v) = \emptyset$, and $U_0(i, v) = 2^{L^+}$. Observe that for all consistent evaluations $E$, $E_0 \leq E$ and hence $E_{s0} \leq E_s$ where $E_{s0}$ and $E_s$ are the suprema of $\sigma(E_0)$ and $\sigma(E)$ resply. Since all suprema are fixed points, $E_{s0}$ is the least fixed point. □

We summarize the results in the following theorem, which provides a base for extending RefL with other inference predicates. We discuss the need for other predicates below, and in Section 5.

**Theorem 1.** *Given the poset of consistent evaluations $(\mathcal{E}, \leq)$ and a function $\mathcal{I} : \mathcal{E} \to \mathcal{E}$ which is inflationary and monotonic, $\mathcal{I}$ has a least fixed point and a maximal fixed point.*

**Discussion:** We now discuss some options in defining conformance, depending on the needs of the application. The sections of the FDA CFR that we have examined can be formalized so that there is a unique fixed point, and conformance is simply the satisfaction of obligations at this fixed point.

However, examples discussed in the literature suggest that it may not be desirable to always have a unique fixed point. A well-known example is that of contrary-to-duty (CTD) obligations [21]. CTD obligations are those that arise when other obligations have been violated. Prakken and Sergot [17] point out an inflexibility in casting CTD structures as an instance of non-monotonic reasoning. We outline how this inflexibility can be avoided, using alternate definitions of conformance. Consider the following example from [15] (similar to one in [17]): *The cottage must not have a fence or a dog. If it has a dog, then it must have both a fence and a warning sign*. The question is what are the obligations when the cottage has a dog. We discuss two possible solutions.

The first solution is to treat the CTD norm as an exception to the first:

1.**o**: $\neg \mathrm{by}_{\{2\}}(f \vee d) \rightsquigarrow \neg(f \vee d)$ and 2.**o**: $d \rightsquigarrow f \wedge w$

The propositions $f$, $d$ and $w$ correpond to the cottage having a fence, dog and warning sign resply. Since there is a dog, the precondition of the second law is true, and this leads to the precondition of the first law being false. So if $f \wedge w$ holds, there is no violation. However, as [17] points out, it may be useful to detect that the situation is worse than the one in which there is no dog. In the second solution, we represent the laws as excluding each other, i.e., we conjoin $\neg \mathrm{by}_{\{1\}}(\neg(f \wedge w))$ to the precondition of the second law. At the least fixed point, both obligations are ungrounded, and we get two maximal fixed points – one in which $\neg(f \vee d)$ is obligated, and one in which $f \wedge w$ is obligated. Since $d$ holds, there is a violation w.r.t. the former fixed point. In a scenario where there is no dog, a unique fixed point is obtained.

Our analysis of CTD structures achieves the same effect as the analyses in [17, 15]. However, [17, 15] characterize the CTD norm as presupposing the violation of the other, and then revising the situation. In future work, we plan to investigate predicates that capture this presuppositional analysis more directly.

### 3.4 Complexity

In this section, we discuss upper and lower bounds for the complexity of conformance checking w.r.t. the least fixed point. Given a run $R$ and regulation $Reg$, we say that $R \models Reg$ iff all obligations are valid in $R$ at the least fixed point. $R$ is assumed to be finite in two ways: (a) The set of objects $O$ is finite, and (b) There exists $n$, such that for all $j \geq n$, $r(n) = r(j)$, i.e., $R$ eventually reaches a stable state.

**Lemma 2 (Upper Bound).** *Given a finite run $R$ and regulation $Reg$, $R \models Reg$ can decided in EXPSPACE (space exponential in the size of $Reg$)*

*Proof.* (sketch) Corollary 1 can easily be turned into a decision procedure. Given an evaluation $E$, it can be shown that $E$ and $\mathcal{I}(E)$ agree on all regulatory preconditions iff

$E$ is a fixed point. So if $E$ is not a fixed point, there exists $i$ and $v$ such that $\mathcal{I}(E)$ has strictly fewer ungrounded preconditions. In the worst case, there is at most one change, and $n \times |Reg| \times |V|$ steps are required to reach a fixed point, where $|V|$ is the number of variable assigments. Note that $|V| = |O|^k$ where $O$ is the set of objects and $k$ is the largest number of distinct variables appearing in a regulatory statement.

To apply $\mathcal{I}$ to an evaluation $E$, we need an explicit representation of the annotation function $\alpha_E$ (for the satisfiablity checks). The worst-case size of the satisfiability instances is $|Reg| \times |O|^k$. Since testing satisifiablity for propositional LTL is PSPACE-complete [19], applying $\mathcal{I}$ requires EXPSPACE (due to the $|O|^k$ factor). We note that for the fragment of LTL discussed in this paper (using only $\Box$ and $\Diamond$) satisfiability is NP-complete [19], and for this fragment $R \models Reg$ can be decided in EXPTIME. $\Box$

**Lemma 3 (Lower Bound).** *Given a finite run $R$ and regulation $Reg$, $R \models Reg$ is hard for EXPTIME (time exponential in the size of $Reg$)*

*Proof.* (sketch) We encode formulas in first-order logic as regulations. Let $\varphi(x_1, ..., x_m)$ be a first-order formula, where $x_1, ..., x_m$ are free variables. If $\varphi(x_1, ..., x_m)$ contains no quantifiers, we represent it by a permission:

$A_\varphi$.**p**: $\varphi(x_1, ..., x_m) \rightsquigarrow q_\varphi(x_1, ..., x_m)$, where $q_\varphi(x_1, ..., x_m)$ is a predicate symbol that doesn't appear in $\varphi(x_1, ..., x_m)$. It is easy to see that $v(q_\varphi(x_1, ..., x_m))$ is available as an annotation iff $\varphi(x_1, ..., x_m)$ is true w.r.t. $v$.

For quantified statements we proceed inductively. Given $\exists y : \varphi(y, x_1, ..., x_m)$, we add two permissions:

$A_{\exists y:\varphi}$.**p**: $\mathrm{by}_{\{\mathrm{A}_\varphi\}}(q_\varphi(y, x_1, ..., x_m)) \rightsquigarrow q'(x_1, ..., x_m)$

$B_{\exists y:\varphi}$.**p**: $\mathrm{by}_{\{\mathrm{A}_{\exists y:\varphi}\}}(q'(x_1, ..., x_m)) \rightsquigarrow q_{\exists y:\varphi}(x_1, ..., x_m)$

Observe that $\mathrm{by}_{\{\mathrm{A}_{\exists y:\varphi}\}}(q'(x_1, ..., x_m))$ is true w.r.t. an assignment $v$ iff $v(q'(x_1, ..., x_m))$ is available as an annotation. And, $v(q'(x_1, ..., x_m))$ is available as an annotation iff $\mathrm{by}_{\mathrm{Id}(\varphi)}(q_\varphi(y, x_1, ..., x_m))$ is true w.r.t. *some* variable assignment $v'$ that is identical to $v$ except for $y$. We can then argue inductively that $v(q_{\exists y:\varphi}(x_1, ..., x_m))$ is available as an annotation iff $\exists y : \varphi(y, x_1, ..., x_m)$ is true w.r.t. $v$.

Given $\forall y : \varphi$, we use the equivalence $\forall y : \varphi = \neg\exists y : \neg\varphi$ and proceed as before. To complete the construction, given $\varphi(x_1, ..., x_m)$, we add the obligation:

1.**o**: $\neg\mathrm{by}_{\{\mathrm{A}_\varphi\}}(q_\varphi(x_1, ..., x_m)) \rightsquigarrow \bot$.

It can be shown that a run with a single state conforms to the regulation iff $\varphi$ is valid at the state. Model-checking for first-order logic is PSPACE-complete (cf. [22]). It follows that computing the least fixed point is PSPACE-hard.

In encoding first-order formulas, we constructed an acyclic regulation. With circular references, one can encode reachability computations which cannot be directly expressed in first-order logic: 1.**p**: $\delta(x, z) \vee (\delta(x, y) \wedge \mathrm{by}_{\{1\}}(\delta^+(y, z))) \rightsquigarrow \delta^+(x, z)$

Here, we assume that each point in a run encodes a graph. The edge relation is given by $\delta$, and $\delta^+$ represents the transitive closure of $\delta$. It can be shown that at the least fixed point $v(\delta^+(x, z))$ is available as an annotation iff there is a path from $v(x)$ to $v(z)$. We can show an EXPTIME lower bound by a reduction from first-order logic enriched with a least fixed point predicate (the system YF in [22]). $\Box$

# 4 Axiomatization

As we discussed in the proof of Lemma 3, RefL contains first order logic enriched with a least fixed point predicate. It follows from results in [23] that the validity problem is $\Pi^1_1$-hard, and as a result, it cannot be recursively axiomatized. We focus on axiomatizing the propositional fragment.

We assume as given a fixed finite domain of quantification, and the variables are replaced by identifiers for domain elements. Given a set of identifiers $ID$, a propositionalized body of regulation has one or more statements of the form $id.\mathbf{x} : \varphi \rightsquigarrow \psi$ for each $id \in ID$. For example, the presence of $id.\mathbf{x} : \varphi_1 \rightsquigarrow \psi_1$ and $id.\mathbf{x} : \varphi_2 \rightsquigarrow \psi_2$ corresponds to different assignments to the variables.

In the presence of multiple fixed points, we can define validity w.r.t. all fixed points, the least fixed point or maximal fixed points. Axiomatizing validity w.r.t. the least or maximal fixed points complicates matters, because we need to distinguish between those formulas that are proved using facts versus those that are proved using inferences. [24] provides an axiomatization of these three notions of validity for default logic, by translating the default rules into an autoepistemic logic. While it may be possible to adapt the translation procedure for RefL, we focus on providing a more direct axiomatization. We axiomatize validity w.r.t. all fixed points, and leave open the proof theory for other notions of validity.

This section is organized as follows. We begin, in Section 4.1, by discussing axioms for the acyclic fragment of RefL. This lets us clarify the central issues, while avoiding complications introduced by three-valued reasoning. We then turn to the general case. Since we have a three valued logic, we will need a different notion of implication. Section 4.2 gives the necessary extensions to the syntax and an alternate definition of semantics to facilitate the proofs. In Section 4.3, we provide an axiomatization using Fitting's sequent calculus [25]. Completeness is proved in Section 4.4. We conclude, in Section 4.5, with example derivations that help clarify the definition of conformance, and show a prototype for the middle value.

## 4.1 The Acyclic Fragment

In this section, we discuss an axiomatization for the fragment of RefL where the references in the regulation are acyclic. This lets us obtain a unique fixed point, and restrict attention to two-valued reasoning. The following axioms and rules characterize propositional and temporal reasoning:

A1 All substitution instances of propositional tautologies
A2 $\Box(\varphi \Rightarrow \psi) \Rightarrow (\Box\varphi \Rightarrow \Box\psi)$
A3 $\Box\varphi \Rightarrow \varphi \wedge \Box\Box\varphi$
R1 From $\vdash \varphi \Rightarrow \psi$ and $\vdash \varphi$, infer $\vdash \psi$
R2 From $\vdash \varphi$ infer $\vdash \Box\varphi$

We characterize the inference predicate by the laws it refers to. To axiomatize $\mathrm{by}_{\mathrm{Id}}(\varphi)$, we need to reason about provability in the language $L$ (propositional LTL). We say that $\varphi \in L$ is is provable (denoted $\vdash_L \varphi$) iff it is an instance of the axioms

A1-A3, or follows from the axioms using the rules R1 and R2. Crucially, we will use the negation of provability in the premise of a rule. Similar mechanisms have been used to axiomatize default logic, e.g., in [24], satisfiability is used in the premise of a rule, and in [26], a modal language is augmented with an operator for satisfiability.

We begin by developing some notation. Given a set of regulatory statements $F = \{id_1.\mathbf{x} : \varphi_1 \rightsquigarrow \psi_1, ..., id_n.\mathbf{x} : \varphi_n \rightsquigarrow \psi_n\}$, let $F_{pre} = \{\varphi_1, ..., \varphi_n\}$ be the set of preconditions, $F_{post} = \{\psi_1, ..., \psi_n\}$ be the set of postconditions, and $F_{id} = \{id_1, ..., id_n\}$ be the set of identifiers. Given a finite set of formulas $\Gamma$, we denote the conjunction by $\bigwedge \Gamma$. The conjunction of the empty set is identified with $\top$ (a tautology). We use two rules for the inference predicate:

R3 For all $F \subseteq Reg$ with $F_{id} \subseteq Id$, from $\vdash_L \bigwedge F_{post} \Rightarrow \phi$, infer $\vdash \bigwedge F_{pre} \Rightarrow \mathrm{by_{Id}}(\phi)$
R4 For all $\psi \in L'$, if for all $F \subseteq Reg$ with $F_{id} \subseteq Id$, either $\nvdash_L \bigwedge F_{post} \Rightarrow \phi$, or $\vdash \psi \Rightarrow \neg \bigwedge F_{pre}$, then infer $\vdash \psi \Rightarrow \neg \mathrm{by_{Id}}(\phi)$.

Informally, R3 says that $\mathrm{by_{Id}}(\phi)$ is true, if there exists a set of laws whose postconditions imply $\phi$, and whose preconditions are true. R4 says that $\mathrm{by_{Id}}(\phi)$ is false, if one of the preconditions is false for all sets of laws whose postconditions imply $\phi$. In particular, if $\nvdash_L \bigwedge F_{post} \Rightarrow \phi$ for all appropriate subsets, then $\vdash \top \Rightarrow \neg \mathrm{by_{Id}}(\phi)$, and using R1, $\vdash \neg \mathrm{by_{id}}(\phi)$.

The rules have an equivalent axiomatic characterization, which is important in establishing completeness. Given $\phi \in L$, let $\mathcal{F}_{(Id,\phi)}$ be the set of subsets ($F \subseteq Reg$ with $F_{id} \subseteq Id$) such that $F \in \mathcal{F}$ iff $\vdash_L \bigwedge F_{post} \Rightarrow \phi$. Let $\Gamma_{(Id,\phi)}$ be the set such that $\neg \bigwedge F_{pre} \in \Gamma_{(Id,\phi)}$ iff $F \in \mathcal{F}_{(Id,\phi)}$. Finally, let $\Delta_{(Id,\phi)}$ be the set such that $\bigwedge F_{pre} \in \Delta_{(Id,\phi)}$ iff $F \in \mathcal{F}_{(Id,\phi)}$.

**Proposition 4.** *The following are provable:*

1. $\vdash \bigwedge \Gamma_{(Id,\phi)} \Rightarrow \neg \mathrm{by_{Id}}(\phi)$
2. $\vdash \mathrm{by_{Id}}(\phi) \Rightarrow \bigvee \Delta_{(Id,\phi)}$

The first claim is an immediate consequence of R4. And, the second claim follows from the first by propositional reasoning. It is easy to show that the axioms A1-A3, together with Proposition 4, and the rules R1 and R2 imply the rules R3 and R4. The inference predicate behaves like a modality:

**Proposition 5.** $\vdash \mathrm{by_{Id}}(\varphi \Rightarrow \psi) \Rightarrow (\mathrm{by_{Id}}(\varphi) \Rightarrow \mathrm{by_{Id}}(\psi))$

We will prove this property in the general setting, in Section 4.3 (Proposition 11). The axioms and rules presented here extend naturally to the three-valued setting. We begin by extending the syntax with the appropriate implication connective for a three-valued logic. We give an alternate definition of the semantics, to facilitate the proofs.

### 4.2 Syntactic and Semantic Preliminaries

We will need two extensions to the syntax of $L^+$. First, we add constants for truth values ($\mathcal{T} = \{\top, ?, \bot\}$). The true values are totally ordered, i.e., $\top > ? > \bot$. Second, we add the natural implication connective $\varphi \supset \psi$.

We now give a different but equivalent definition of the semantics, to facilitate the proofs. A run $R = (r, \pi)$ is a pair, where $r$ is a sequence of states, and $\pi$ is a truth assignment to atomic propositions. Statements in $L$ (propositional LTL) are evaluated at points $(R, i)$. We define $\mathrm{val}(\varphi, R, i)$ inductively as follows:

- $\mathrm{val}(p, R, i) = \top$ iff $p \in \pi(r(i))$. Otherwise, $\bot$.
- Conjunction and negation are defined in the usual way
- $\mathrm{val}(\varphi \supset \psi, R, i) = t$, where $t$ is the greatest truth value such that $\mathrm{val}(\varphi, R, i) \wedge t \leq \mathrm{val}(\psi, R, i)$. Since statements in $L$ are two valued, $\varphi \supset \psi \equiv \varphi \Rightarrow \psi$.
- $\mathrm{val}(\Box\varphi, R, i) = \bigwedge\{\mathrm{val}(\varphi, R, j) \mid j \geq i\}$

We say that $\varphi \in L$ is valid iff for all points $(R, i)$, we have $\mathrm{val}(\varphi, R, i) = \top$. For statements in $L^+$, in addition to a point $(R, i)$, we need two annotation functions $(\alpha, \alpha')$. We define $\mathrm{val}_{(\alpha,\alpha')}$ as follows:

- $\mathrm{val}_{(\alpha,\alpha')}(t, R, i) = t$ for $t \in \mathcal{T}$
- $\mathrm{val}_{(\alpha,\alpha')}(\mathrm{by}_{\mathrm{Id}}(\varphi), R, i) = \top$ if $\bigwedge \alpha.Id(i) \supset \varphi$ is valid
  $\mathrm{val}_{(\alpha,\alpha')}(\mathrm{by}_{\mathrm{Id}}(\varphi), R, i) = ?$ if $\bigwedge \alpha'.Id(i) \supset \varphi$ is valid
  $\mathrm{val}_{(\alpha,\alpha')}(\mathrm{by}_{\mathrm{Id}}(\varphi), R, i) = \bot$ otherwise
- For all other formulas the definition is as before. In the three-valued setting $\varphi \supset \psi$ and $\varphi \Rightarrow \psi$ are not identical.

We say that $(\alpha, \alpha')$ is *a fixed point* for a run $R$ iff for all $i \in N$ and $id.\mathbf{x} : \varphi \rightsquigarrow \psi$:

- id: $\psi \in \alpha(i)$ iff $\mathrm{val}_{(\alpha,\alpha')}(\varphi, R, i) = \top$
- id: $\psi \in \alpha'(i)$ iff $\mathrm{val}_{(\alpha,\alpha')}(\varphi, R, i) \geq ?$

It follows that for all $i \in N$, $\alpha(i) \subseteq \alpha'(i)$. We now define satisfiability and validity at a point:

- $\varphi$ is satisfiable at $(R, i)$ iff $val_{(\alpha,\alpha')}(\varphi, R, i) = \top$ for some fixed point $(\alpha, \alpha')$
- $\varphi$ is valid at $(R, i)$ iff $val_{(\alpha,\alpha')}(\varphi, R, i) = \top$ for all fixed points $(\alpha, \alpha')$

Finally, we say that $\varphi$ is valid iff $\varphi$ is valid at all points. We are now ready to axiomatize RefL.

### 4.3 Sequent Calculus

We use Fitting's sequent calculus [25]. A sequent is a statement of the form $\Gamma \rightarrow \Delta$, where $\Gamma$ and $\Delta$ are finite sets of *implications*. A sequent is valid at a point $(R, i)$ iff for all fixed points $(\alpha, \alpha')$, either $\mathrm{val}_{(\alpha,\alpha')}(X, R, i) \neq \top$ for some $X \in \Gamma$, or $\mathrm{val}_{(\alpha,\alpha')}(X, R, i) = \top$ for some $X \in \Delta$. A sequent is valid iff it is valid at all points. Following [25], we use lower case letters for truth values, and upper case letters for formulas.

We begin by reviewing the axioms and rules for propositional and temporal reasoning. All the rules are given in [25]. We introduce some additional axioms for negation and the temporal operators.

**Basic Axioms and Rules**:

$$X \to X$$

$$\frac{\Gamma \to \Delta}{\Gamma \cup \Gamma' \to \Delta \cup \Delta'}\text{(thinning)}$$

$$\frac{\Gamma \to \Delta, X \qquad \Gamma, X \to \Delta}{\Gamma \to \Delta}\text{(cut)}$$

$$A \supset B, B \supset C \to A \supset C$$

**Truth Value Axioms and Rules:**

$$\frac{\Gamma, t \supset A \to \Delta, t \supset B \qquad (\forall t \in \mathcal{T})}{\Gamma \to \Delta, A \supset B}(t \supset)$$

$$\frac{\Gamma, B \supset t \to \Delta, A \supset t \qquad (\forall t \in \mathcal{T})}{\Gamma \to \Delta, A \supset B}(\supset t)$$

$$\to a \supset b \qquad if\ a \leq b$$

$$a \supset b \to \qquad if\ a \not\leq b$$

$$\to \top \supset p, p \supset \bot \qquad (\text{for all atomic propositions p})$$

The last axiom ensures that LTL formulas are either true or false. The middle value arises only due to the inference predicate.

**Proposition 6.** *The following are provable:*
$\to A \supset \top$
$\to \bot \supset A$
$\to A \supset A$

*Proof.* We prove the first claim:

$$\frac{\dfrac{\to t \supset \top}{t \supset A \to t \supset \top}\text{(thinning)}}{\to A \supset \top}(t \supset)$$

□

In [25] and here, the proof of completeness makes crucial use of a derived rule:

**Proposition 7 ([25]).** *The following is a derived rule:*

$$\frac{\Gamma, A \supset t, t \supset A \to \Delta \qquad (\forall t \in \mathcal{T})}{\Gamma \to \Delta}$$

*Proof.* [25] gives a proof of this derived rule for any finite lattice. We use the fixed lattice to give a simpler proof. We are given that $\Gamma, A \supset \top, \top \supset A \rightarrow \Delta$. By Proposition 6, $\rightarrow A \supset \top$. Using cut, we get $\Gamma, \top \supset A \rightarrow \Delta$. We can now derive:

$$\dfrac{\dfrac{\Gamma, \top \supset A \rightarrow \Delta \qquad \top \supset ?, ? \supset A \rightarrow \top \supset A}{\Gamma \rightarrow \Delta, \top \supset ?, ? \supset A}(\text{cut}) \qquad \top \supset ? \rightarrow}{\Gamma \rightarrow \Delta, ? \supset A}(\text{cut})$$

Similarly, we can derive $\Gamma \rightarrow \Delta, A \supset ?$ from $\Gamma, A \supset \bot, \bot \supset A \rightarrow \Delta$. Then, given $\Gamma, A \supset ?, ? \supset A \rightarrow \Delta$, two applications of cut gives us $\Gamma \rightarrow \Delta$. □

**Conjunction Axioms**:

$$\rightarrow A \wedge B \supset A$$

$$\rightarrow A \wedge B \supset B$$

$$C \supset A, C \supset B \rightarrow C \supset A \wedge B$$

**Negation Axioms**:

$$\rightarrow A \supset \neg\neg A$$

$$\rightarrow \neg\neg A \supset A$$

$$A \supset B \rightarrow \neg B \supset \neg A$$

$$\rightarrow a \supset \neg b \qquad (a = \neg b)$$

$$\rightarrow \neg b \supset a \qquad (a = \neg b)$$

**Implication Axioms**: We treat implication as right associative, i.e., $A \supset B \supset C \equiv A \supset (B \supset C)$.

$$A \wedge B \supset C \rightarrow A \supset B \supset C$$

$$A \supset B \supset C \rightarrow A \wedge B \supset C$$

We now establish some useful facts about implications, which are useful in deriving properties of modalities:

**Proposition 8.** *The following are provable:*

$$A \supset B \rightarrow t \supset A \supset B$$

$$\top \supset A \supset B \rightarrow A \supset B$$

$$t \supset A \supset B, t \supset A \rightarrow t \supset B$$

*Proof.* For the first claim:

$$\frac{t \wedge A \supset A, A \supset B \rightarrow t \wedge A \supset B \qquad \rightarrow t \wedge A \supset A}{A \supset B \rightarrow t \wedge A \supset B}\text{(cut)}$$

Now we can derive:

$$\frac{A \supset B \rightarrow t \wedge A \supset B \qquad t \wedge A \supset B \rightarrow t \supset A \supset B}{A \supset B \rightarrow t \supset A \supset B}\text{(cut)}$$

For the second claim, we need the observation that $\rightarrow A \supset \top \wedge A$ is provable:

$$\frac{A \supset \top, A \supset A \rightarrow A \supset \top \wedge A \qquad \rightarrow A \supset \top \qquad \rightarrow A \supset A}{\rightarrow A \supset \top \wedge A}\text{(2 cuts)}$$

$$\frac{A \supset \top \wedge A, \top \wedge A \supset B \rightarrow A \supset B \qquad \rightarrow A \supset \top \wedge A}{\top \wedge A \supset B \rightarrow A \supset B}\text{(cut)}$$

Now using the axiom $\top \supset A \supset B \rightarrow \top \wedge A \supset B$, an application of cut gives us $\top \supset A \supset B \rightarrow A \supset B$.

Finally, for the third claim, we need the observation that $\rightarrow (A \supset B) \wedge A \supset B$ is provable. By Proposition 6, $\rightarrow A \supset A$, and so, $\rightarrow (A \supset B) \supset A \supset B$. Using the implication axiom $(A \supset B) \supset A \supset B \rightarrow (A \supset B) \wedge A \supset B$, an application of cut gives us the desired result.

$$\frac{t \supset (A \supset B) \wedge A, (A \supset B) \wedge A \supset B \rightarrow t \supset B \qquad \rightarrow (A \supset B) \wedge A \supset B}{t \supset (A \supset B) \wedge A \rightarrow t \supset B}$$

$$\frac{t \supset A \supset B, t \supset A \rightarrow t \supset (A \supset B) \wedge A \qquad t \supset (A \supset B) \wedge A \rightarrow t \supset B}{t \supset A \supset B, t \supset A \rightarrow t \supset B}$$

□

**Temporal Reasoning**:

$$\frac{a_1 \supset A_1, ..., a_n \supset A_n \rightarrow b \supset B \qquad (n \geq 0)}{a_1 \supset \Box A_1, ..., a_n \supset \Box A_n \rightarrow b \supset \Box B}\text{(TNecc)}$$

$$\rightarrow \Box A \supset A \wedge \Diamond A \wedge \Box\Box A$$

We can now prove the distribution axiom:

**Proposition 9.** *The following is provable:*

$$\rightarrow \Box(A \supset B) \supset \Box A \supset \Box B$$

*Proof.* By Proposition 8, $t \supset A \supset B, t \supset A \rightarrow t \supset B$. Using TNecc, we get $t \supset \Box(A \supset B), t \supset \Box A \rightarrow t \supset \Box B$. It is easy to derive:

$t \supset \Box(A \supset B) \wedge \Box A \rightarrow t \supset \Box B$

Using the rule $(t \supset)$, we get $\rightarrow \Box(A \supset B) \wedge \Box A \supset \Box B$. The desired result follows using the implication axiom. □

**Rules for the Inference Predicate**:

We now introduce two rules for the inference predicate, analogous to the rules that we discussed in Section 4.1. We begin with a semantic characterization.

Given a set of regulatory statements $F = \{id_1.\mathbf{x}: \ A_1 \rightsquigarrow B_1, ..., id_n.\mathbf{x}: \ A_n \rightsquigarrow B_n\}$, let $F_{pre} = \{A_1, ...A_n\}$ be the set of preconditions, $F_{post} = \{B_1, ..., B_n\}$ be the set of postconditions, and $F_{id} = \{id_1, ..., id_n\}$ be the set of identifiers.

Given a set of identifiers $Id$, let $Reg_{Id}$ be the set of subsets of regulatory statements $F$ such that $F_{id} \subseteq Id$. Given $C \in L$, let $Reg_{(Id,C)}$ be the sets $F \in Reg.Id$ such that $\bigwedge F_{post} \supset C$ is valid. Given a point $(R, i)$ and a fixed point $(\alpha, \alpha')$:

$$\mathrm{val}_{(\alpha,\alpha')}(\mathrm{by}_{\mathrm{Id}}(C), R, i) = \bigvee \left\{ \mathrm{val}_{(\alpha,\alpha')}(\bigwedge F_{pre}, R, i) | F \in Reg_{(Id,C)} \right\}$$

In other words, $\mathrm{by}_{\mathrm{Id}}(C)$ is true iff there is a set of laws ($F$ with $F_{id} \subseteq Id$) such that (a) $C$ can be inferred from the postconditions, and (b) the preconditons are true. Similarly, $\mathrm{by}_{\mathrm{Id}}(C)$ is false iff for all appropriate sets of laws such that $C$ can be inferred from the postconditions, one of the preconditions is false.

To axiomatize $\mathrm{by}_{\mathrm{Id}}(C)$, we need to reason about provability in the language $L$ (propositional LTL). We say that a sequent in the language $L$ is provable (denoted $\Gamma \rightarrow_L \Delta$) iff it is provable using the axioms and rules introduced previously. As we discussed in Section 4.1, we will need to use the negation of provability in the premise of a rule. The rules are as follows:

$$\frac{F = \{id_1.\mathbf{x}: \ A_1 \rightsquigarrow B_1, ..., id_n.\mathbf{x}: \ A_n \rightsquigarrow B_n\} \subseteq Reg, F_{id} \subseteq Id \quad \rightarrow_L B_1 \wedge ... \wedge B_n \supset C}{t \supset A_1, ..., t \supset A_n \rightarrow t \supset \mathrm{by}_{\mathrm{Id}}(C)} \text{(RBy1)}$$

$$\frac{\begin{array}{c} For\ all\ F = \{id_1.\mathbf{x}: \ A_1 \rightsquigarrow B_1, ..., id_n.\mathbf{x}: \ A_n \rightsquigarrow B_n\} \subseteq Reg, F_{id} \subseteq Id \\ If \ \rightarrow_L B_1 \wedge ... \wedge B_n \supset C \ then \ \Gamma \rightarrow A_1 \supset t, ..., A_n \supset t \end{array}}{\Gamma \rightarrow \mathrm{by}_{\mathrm{Id}}(C) \supset t} \text{(RBy2)}$$

Informally, RBy1 says that $\mathrm{by}_{\mathrm{Id}}(C)$ is true, if there exists $F \in Reg_{(Id,C)}$ such that the preconditions are true. RBy2 says that $\mathrm{by}_{\mathrm{Id}}(C)$ is false, if one of the preconditions is false (for all $F \in Reg_{(Id,C)}$). In particular, if $\rightarrow_L B_1 \wedge ... \wedge B_n \supset C$ is not provable for all appropriate subsets, then $\rightarrow \mathrm{by}_{\mathrm{Id}}(C) \supset \bot$, as the premise of RBy2 is vacuously satisfied.

We now develop some notation that is useful in several subsequent proofs. Given $C \in L$, let $\mathcal{F}_{(Id,C)}$ be the set of subsets ($F \subseteq Reg$ with $F_{id} \subseteq Id$) such that $F \in \mathcal{F}$ iff $\rightarrow_L \bigwedge F_{post} \supset C$. Let $\Delta_{(Id,C)}(t)$ be the set such that $t \supset \bigwedge F_{pre} \in \Delta_{(Id,C)}(t)$ iff

$F \in \mathcal{F}_{(Id,C)}$. Finally, let $\Gamma_{(Id,C)}(t)$ be the set such that $\bigwedge F_{pre} \supset t \in \Gamma_{(Id,C)}(t)$ iff $F \in \mathcal{F}_{(Id,C)}$.

**Proposition 10.** *The following are provable:*

$$\Gamma_{(Id,C)}(t) \rightarrow \mathrm{by}_{\mathrm{Id}}(C) \supset t$$

$$t \supset \mathrm{by}_{\mathrm{Id}}(C) \rightarrow \Delta_{(Id,C)}(t)$$

*Proof.* The first claim is immediate from RBy2. For the second claim, we show the proof for $t = \top$. By propositional reasoning, the following is provable:

$$\rightarrow \top \supset A, A \supset ? \qquad (\forall A \in L^+)$$

From the first claim, $\Gamma_C(?) \rightarrow \mathrm{by}_{\mathrm{Id}}(C) \supset ?$, and it follows that:

$$\top \supset \mathrm{by}_{\mathrm{Id}}(C), \Gamma_C(?) \rightarrow$$

For each $A \supset ? = X$ such that $X \in \Gamma_C(?)$, we have $\rightarrow \top \supset A, X$. Using cut, we get:

$$\top \supset \mathrm{by}_{\mathrm{Id}}(C), \Gamma_C(?) - \{X\} \rightarrow \top \supset A$$

Since $\Gamma_C(?)$ is finite, repeated applications of cut will give us:

$$\top \supset \mathrm{by}_{\mathrm{Id}}(C) \rightarrow \Delta_C(\top)$$

□

We can show that the inference predicate behaves like a modality, by deriving a weaker version of the necessitation rule:[1]

**Proposition 11.** *The following is a derived rule:*

$$\frac{\rightarrow_L D_1 \wedge ... \wedge D_n \supset C}{\rightarrow \mathrm{by}_{\mathrm{Id}}(D_1) \wedge ... \wedge \mathrm{by}_{\mathrm{Id}}(D_n) \supset \mathrm{by}_{\mathrm{Id}}(C)}$$

*Proof.* By Proposition 10, $t \supset \mathrm{by}_{\mathrm{Id}}(D_i) \rightarrow \Delta_{(Id,D_i)}(t)$ is provable for $1 \leq i \leq n$. We construct $\Delta$ such that for each $t \supset A_i \in \Delta_{(Id,D_i)}(t)$, we have $t \supset A_1 \wedge ... \wedge A_n \in \Delta$. By propositional reasoning, it follows that:

$$t \supset \mathrm{by}_{\mathrm{Id}}(D_1), ..., t \supset \mathrm{by}_{\mathrm{Id}}(D_n) \rightarrow \Delta$$

Observe that each $X \in \Delta$ is associated with a set of regulatory statements $F$, such that $F_{id} \subseteq Id$ and $\rightarrow_L \bigwedge F_{post} \supset D_i$ for all $1 \leq i \leq n$. Using the fact that

[1] The stronger version of the necessitation rule (schematically equivalent to TNecc) can be derived by making use of the two valued restriction of LTL. However, we have not found an appropriate generalization for a many-valued logic.

$\rightarrow_L D_1 \wedge ... \wedge D_n \supset C$, it is easy to show that $\rightarrow_L \bigwedge F_{post} \supset C$. Then RBy1 gives us $X \rightarrow t \supset \mathrm{by}_{\mathrm{Id}}(C)$ for all $X \in \Delta$. Repeated applications of cut will give us:

$$t \supset \mathrm{by}_{\mathrm{Id}}(D_1), ..., t \supset \mathrm{by}_{\mathrm{Id}}(D_n) \rightarrow t \supset \mathrm{by}_{\mathrm{Id}}(C)$$

The desired result follows using propositional reasoning. The distribution axiom, i.e., $\rightarrow \mathrm{by}_{\mathrm{Id}}(A \supset B) \supset \mathrm{by}_{\mathrm{Id}}(A) \supset \mathrm{by}_{\mathrm{Id}}(B)$ follows easily using this derived rule, and the fact that $\rightarrow_L (A \supset B) \wedge A \supset B$. □

### 4.4 Completeness

We now discuss the soundness and completeness of the type system. Soundness, as usual, is straightforward, and we leave the details to the reader. We begin by showing completeness for the atemporal fragment. From the perspective of a temporal operator, a formula $\mathrm{by}_{\mathrm{Id}}(C)$ is simply an atomic proposition which can have the middle value. We use the pre-model construction in [27] to generalize the proof to a temporal setting.

Given an implication $X$, let $sub(X)$ be the set of subformulas of $X \cup Reg$ and their negations. Note that the subformulas of $Reg$ are the subformulas of the preconditions and postconditions. $\neg\neg A$ is identified with $A$. Given $sub(X)$, we construct the set of implications $cl(X)$ such that for all $A \in sub(X)$ and $t \in \mathcal{T}$ $\{A \supset t, t \supset A\} \subseteq cl(X)$.

**Definition 13.** *Given $\Gamma \subseteq cl(X)$ and $Y \in cl(X)$:*

- *$\Gamma$ is $Y$-consistent iff $\Gamma \rightarrow Y$ is not provable. $\Gamma$ is $Y$-inconsistent iff $\Gamma \rightarrow Y$ is provable.*
- *$\Gamma$ is maximal $Y$-consistent iff $\Gamma$ is $Y$-consistent and for all $Z \in cl(X) - \Gamma$, $\Gamma \cup \{Z\}$ is $Y$-inconsistent*

**Theorem 2 ([25]).** *Given $\Gamma \subseteq cl(X)$ and $Y \in cl(X)$ such that $\Gamma$ is maximal $Y$-consistent, for all $A \in cl(X)$, there is exactly one $t \in \mathcal{T}$ such that $\{t \supset A, A \supset t\} \subseteq \Gamma$*

*Proof.* We first show that for each $A \in cl(X)$ there is at most one truth value with the requisite properties. Suppose not. The we have two truth values such that $\{t_1 \supset A, A \supset t_1\} \subseteq \Gamma$ and $\{t_2 \supset A, A \supset t_2\} \subseteq \Gamma$. It is easy to derive that $\Gamma \rightarrow t_1 \supset t_2$ and $\Gamma \rightarrow t_2 \supset t_1$. Since $t_1 \neq t_2$, either $t_1 \not\leq t_2$ or $t_2 \not\leq t_1$. So, by the truth value axioms we have either $t_1 \supset t_2 \rightarrow$ or $t_2 \supset t_1 \rightarrow$. In either case, using cut, $\Gamma \rightarrow$ is provable, and by thinning, $\Gamma \rightarrow Y$ is provable. This contradicts the $Y$-consistency of $\Gamma$.

Now we show that there is at least one truth value with the requisite properties. Suppose not. Since $\Gamma$ is maximal, we have:

$$\Gamma, A \supset t, t \supset A \rightarrow Y \qquad (\forall t \in \mathcal{T})$$

By Proposition 7, it follows that $\Gamma \rightarrow Y$, contradicting the $Y$-consistency of $\Gamma$. □

**Lemma 4.** *Given $\Gamma \subseteq cl(X)$ and $Y \in cl(X)$ such that $\Gamma$ is maximal $Y$-consistent and $\mathrm{by}_{\mathrm{Id}}(C) \in cl(X)$:*

*$t \supset \mathrm{by}_{\mathrm{Id}}(C) \in \Gamma$ iff there exists $F \in \mathcal{F}_{(Id,C)}$ such that for all $A \in F_{pre}$, $t \supset A \in \Gamma$*
*$\mathrm{by}_{\mathrm{Id}}(C) \supset t \in \Gamma$ iff for all $F \in \mathcal{F}_{(Id,C)}$, there exists $A \in F_{pre}$ and $A \supset t \in \Gamma$.*

For each part, one direction follows directly from the inference rules, and the other direction follows directly from Proposition 10.

Given a maximal $X$-consistent set $\Gamma$, we construct a state $s_\Gamma$ such that for all atomic propositions $p$, $p \in s_\Gamma$ iff $\{\top \supset p, p \supset \top\} \subseteq \Gamma$. We also construct sets $\alpha_\Gamma$ and $\alpha'_\Gamma$ such that for each $id.\mathbf{x}: \ A \rightsquigarrow B \in Reg$:

- id: $B \in \alpha_\Gamma$ iff $\{\top \supset A, A \supset \top\} \subseteq \Gamma$
- id: $B \in \alpha'_\Gamma$ iff id: $B \in \alpha_\Gamma$ or $\{? \supset A, A \supset ?\} \subseteq \Gamma$

The completeness proof is finished in the usual way. $s_\Gamma$ is extended into a run $R$ with a single state. A single state suffices for the atemporal case. $(\alpha_\Gamma, \alpha'_\Gamma)$ are extended to annotation functions $(\alpha, \alpha')$. It is easy to show that $\mathrm{val}_{(\alpha,\alpha')}(A, R, i) = t$ iff $t$ is the unique value such that $\{A \supset t, t \supset A\} \subseteq \Gamma$. Using Lemma 4 and the construction of annotation functions, we can argue that the annotations correspond to a fixed point. Thus if $\rightarrow X$ is not provable, we can create a maximal $\top \supset X$-consistent set $\Gamma$, which is extended to a run and fixed point such that $X$ is not true.

Now, we consider the temporal case. Given $X \in L^+$ and a body of regulation, let $M_X$ be the set of all maximal consistent sets, i.e., $\Gamma \in M_X$ iff $\Gamma$ is maximal $Y$-consistent for some $Y \in cl(X)$. We construct the relation $\delta_X \subseteq M \times M$ such that $(\Gamma, \Gamma') \in \delta_X$ iff for all temporal formulas $\Box A \in sub(X)$, if $t \supset \Box A \in \Gamma$, then $\{t \supset A, t \supset \Box A\} \subseteq \Gamma'$. Intuitively, the graph of maximal consistent sets $G_X = (M_X, \delta_X)$ encodes a set or runs. The global formulas ($t \supset \Box A$) get the right interpretation, but not so for eventual formulas ($\Box A \supset t$). We will be interested in the set of paths which are *fulfilling* [27]:

**Definition 14.** *Given $X \in L^+$ and $G_X = (M_X, \delta_X)$, a path in $G_X$ is an infinite sequence of states $p_X : N \rightarrow M_X$, such that for all $i \in N$, $(r(i), r(i+1)) \in \delta_X$. A path $p_X$ is said to be fulfilling iff for all temporal formulas $\Box A \in sub(X)$ and for all $i \in N$, if $\Box A \supset t \in r(i)$, then there exists $j \geq i$ such that $A \supset t \in r(j)$.*

We now prove the existence of fulfilling paths:

**Lemma 5.** *Given $X \in L^+$ and $G_X = (M_X, \delta_X)$, for all $\Gamma \in M_X$, $\Box A \supset t \in \Gamma$ iff there exists a finite path $(\Gamma_0, ..., \Gamma_n)$ such that $\Gamma_0 = \Gamma$, for all $0 \leq i < n$, $(\Gamma_i, \Gamma_{i+1}) \in \delta$ and $A \supset t \in \Gamma_n$.*

*Proof.* Suppose $\Box A \supset t \in \Gamma$, and no appropriate finite sequence exists. Let $T_\Gamma \subseteq M_X$ be the smallest set such that (a) $\Gamma \in T_\Gamma$, and (b) if $\Gamma_1 \in T_\Gamma$ and $(\Gamma_1, \Gamma_2) \in \delta_X$, then $\Gamma_2 \in T_\Gamma$. In other words, $T_\Gamma$ is the set of states reachable from $\Gamma$. Observe that for all $\Gamma' \in T_\Gamma$, $A \supset t \notin \Gamma'$. Since the sets in $T_\Gamma$ are maximal, there exists some $t' \not\leq t$, such that for all $\Gamma' \in T_\Gamma$, $t' \supset A \in \Gamma'$. Consider the set of implications $\{t_1 \supset \Box A_1, ..., t_n \supset \Box A_n\} \subseteq \Gamma$. We claim that:

$$t_1 \supset \Box A_1, ..., t_n \supset \Box A_n, t_1 \supset A_1, ..., t_n \supset A_n \rightarrow t' \supset A$$

For if not, we can construct a maximal $t' \supset A$-consistent set $\Gamma''$ such that $\Gamma'' \in T_\Gamma$. But, this contradicts the fact that $t' \supset A \in \Gamma'$ for all $\Gamma' \in T_\Gamma$. Assuming that the sequent above is provable, using TNecc, we get:

$$t_1 \supset \Box\Box A_1, ..., t_n \supset \Box\Box A_n, t_1 \supset \Box A_1, ..., t_n \supset \Box A_n \rightarrow t' \supset \Box A$$

Using the fact that $\rightarrow \Box A \supset \Box\Box A$, we can derive that:

$$t_1 \supset \Box A_1, ..., t_n \supset \Box A_n \rightarrow t' \supset \Box A$$

Since all items on the left are in $\Gamma$, $t' \supset \Box A \in \Gamma$. However, $t' \not\leq t$ and $\Box A \supset t \in \Gamma$, from which we can contradict the fact that $\Gamma$ is consistent. As a result, there exists $\Gamma' \in T_\Gamma$ such that $A \supset t \in \Gamma'$. Since $M_X$ is finite, there exists a finite path from $\Gamma$ to $\Gamma'$.

For the other direction, suppose we are given a finite path $(\Gamma_0, ..., \Gamma_n)$ such that $A \supset t \in \Gamma_n$. We need to show that $\Box A \supset t \in \Gamma_0$. The proof proceeds by induction on $n$. For $n = 0$, we have $\Gamma_0 \rightarrow A \supset t$. Since $\rightarrow \Box A \supset A$, we can derive that $\Gamma_0 \rightarrow \Box A \supset t$. For $n = 1$, we have $\Gamma_1 \rightarrow A \supset t$. Suppose $\Box A \supset t \notin \Gamma_0$, we have $\Gamma_0 \rightarrow t' \supset \Box A$ for some $t' \not\leq t$. So, $\Gamma_1 \rightarrow t' \supset A$ contradicting the consistency of $\Gamma_1$. For the inductive set, since $\Gamma_n \rightarrow A \supset t$, we have $\Gamma_1 \rightarrow \Box A \supset t$ (by induction hypothesis). Again, suppose $\Box A \supset t \notin \Gamma_0$, we have $\Gamma_0 \rightarrow t' \supset \Box A$ for some $t' \not\leq t$. So, $\Gamma_1 \rightarrow t' \supset \Box A$ contradicting the consistency of $\Gamma_1$. □

Completeness is established analogously to the atemporal setting. Given $X \in L^+$ such that $\rightarrow X$ is not provable, we construct $G_X = (M_X, \delta_X)$. Observe that there exists $\Gamma \in M_X$ such that $\Gamma$ is $\top \supset X$-consistent. Using Lemma 5, construct a fulfilling path $p_X : N \rightarrow M_X$ such that $p_X(0) = \Gamma$. The path is extend to a run $R$ with fixed point annotations $(\alpha, \alpha')$, as discussed earlier. It is easy to show that $\mathrm{val}_{(\alpha,\alpha')}(A, R, i) = t$ iff $t$ is the unique value such that $\{A \supset t, t \supset A\} \subseteq \Gamma$. As a result, $\mathrm{val}_{(\alpha,\alpha')}(X, R, 0) \neq \top$, and $X$ is not valid. We obtain the following:

**Theorem 3.** *Given a body of regulation $Reg$, for all implications $X \in L^+$:*
*$\rightarrow X$ is provable iff $X$ is valid*

### 4.5 Example Derivations

We discuss two examples. The first example will be used to clarify our definition of conformance, and the second to show a prototype for the middle value.
**Example 1**: Consider the propositionalized version of our regulatory sentences:

- 1.**o**: $d \wedge \neg \mathrm{by}_{\{2\}}(\neg\Diamond test) \rightsquigarrow \Diamond test$
- 2.**p**: $sp \rightsquigarrow \neg\Diamond test$

The following is provable:

$$\rightarrow d \wedge \neg sp \supset \mathrm{by}_{\{1\}}(\Diamond test)$$

Since $\top \supset \neg\Diamond test$ is satisfiable, $\rightarrow_L \top \supset \Diamond test$ is not provable. By Proposition 6, we have $\rightarrow \neg\Diamond test \supset \neg\Diamond test$. By Proposition 10, we get:

$$sp \supset t \rightarrow \mathrm{by}_{\{2\}}(\neg\Diamond test) \supset t \qquad (*)$$

Since $\rightarrow_L \Diamond test \supset \Diamond test$, it follows from RBy1 that:

$$t \supset d \wedge \neg \mathrm{by}_{\{2\}}(\neg\Diamond test) \rightarrow t \supset \mathrm{by}_{\{1\}}(\Diamond test) \qquad (**)$$

The result follows easily from propositional reasoning. From $(*)$, using $(\supset t)$, we get $\rightarrow \text{by}_{\{2\}}(\neg\Diamond test) \supset sp$. Using the negation axiom, we get:

$$\rightarrow \neg sp \supset \neg\text{by}_{\{2\}}(\neg\Diamond test)$$

By Propositon 8, we have $A \supset B \rightarrow t \supset A \supset B$ and $t \supset A \supset B, t \supset A \rightarrow t \supset B$. We can derive that:

$$t \supset \neg sp \rightarrow t \supset \neg\text{by}_{\{2\}}(\neg\Diamond test) \qquad (***)$$

Now using $(**)$, we can derive $t \supset d, t \supset \neg\text{by}_{\{2\}}(\neg\Diamond test) \rightarrow t \supset \text{by}_{\{1\}}(\Diamond test)$. Using $(***)$, an application of cut gives us:

$$t \supset d, t \supset \neg sp \rightarrow t \supset \text{by}_{\{1\}}(\Diamond test)$$

It is easy to show that $t \supset (d \wedge sp) \rightarrow t \supset d$ and $t \supset (d \wedge \neg sp) \rightarrow t \supset \neg sp$. Two applications of cut gives us $t \supset d \wedge \neg sp \rightarrow t \supset \text{by}_{\{1\}}(\Diamond test)$. Now applying $(t \supset)$:

$$\rightarrow d \wedge \neg sp \supset \text{by}_{\{1\}}(\Diamond test)$$

What does this tell us about conformance? Intuitively, regulations tell us nothing about what actually holds. Given the regulation above, $\rightarrow d \wedge \neg sp \supset \Diamond test$ is not provable. Conformance is a separate notion of inference, i.e., *what is required is true*. Given a body of regulation let $Id_{\mathbf{o}}$ be the identifiers of the obligations. The actual state of affairs can be given by a run, or described declaratively by a set of LTL formulas $\Gamma$. The idea is that $\Gamma$ conforms to the regulation iff for all implications $X \in L$ such that $\Gamma \rightarrow \top \supset \text{by}_{\text{Id}_{\mathbf{o}}}(X)$, we have $\Gamma \rightarrow X$.

**Example 2**: The following regulation gives us a prototype for the middle value:

– 1.**o**: $\neg\text{by}_{\{1\}}(p) \rightsquigarrow p$

This obligation requires $p$ when it doesn't require p and is always ungrounded. The following are provable:

$$\rightarrow \text{by}_{\{1\}}(p) \supset ?$$

$$\rightarrow ? \supset \text{by}_{\{1\}}(p)$$

Using RBy1, RBy2 and Proposition 10, it is easy to show that $\rightarrow \text{by}_{\{1\}}(p) \supset \neg\text{by}_{\{1\}}(p)$ and $\rightarrow \neg\text{by}_{\{1\}}(p) \supset \text{by}_{\{1\}}(p)$. By propositional reasoning, it is easy to show that $A \supset \neg A, \neg A \supset A \rightarrow A \supset ?$ and $A \supset \neg A, \neg A \supset A \rightarrow ? \supset A$. The provability of the claims follows easily.

## 5 Conclusions and Future Work

We have motivated and described a logic (RefL) that accomodates references between laws. RefL separates two uses of statements – drawing inferences from regulation, and determining facts about an organization. We believe that this separation is crucial to the application of conformance checking.

The inference predicate blends two ideas from logic programming. First, the Kripke-Kleene-Fitting semantics [28], which uses three values for negation in logic programs. In RefL, we place the burden on a predicate, rather than on negation. The advantage is that connectives can behave as they do in a many valued logic. Second, contextual logic programs [29] use operations to restrict the context from which inferences are derived. Referring to specific laws (via identifiers) gives us a fine-grained control of context.

RefL provides a staring point in bringing the advantages of non-monotonic reasoning to systems such as [3, 5]. [3] represents business contracts as SQL queries, and [5] uses first-order logic augmented with real time operators. The inference predicate can be added to these systems, provided that the existential quantification is relativized to either the preconditions or the postconditions. However, restrictions are needed to ensure that the satisfiability tests remain decidable. [4] discusses the importance of anlayzing references, but do not provide a formalization.

In this work, we have considered references to laws that appear in preconditions. There is also the need for references in postconditions. An obvious case is for laws that cancel obligations and permissions given by another, e.g., *if a donation is not used for transfusion, exemption (3) no longer applies.* A more speculative case can be made for iterated deontic constructs [18], e.g., "required to allow x". We suggest that the semantics will involve representing agents who introduce laws that reason about each other, e.g., *You are required to (introduce laws that) allow a patient to see his records*.

On the computational side, our goal is to be able to scale up to runs with a large number of objects, and incorporate RefL into a runtime checking framework for LTL. In a companion paper [30], we identify a fragment of RefL motivated by a case study of the FDA CFR. The fragment assumes that $\mathrm{by}_{\mathrm{Id}}(\varphi)$ can be evaluated by using at most one of the laws referred to. This assumption allows us to replace satisfiability tests with tests of lower complexity, and lets us scale up to runs with a large number of objects. In this paper, we have focussed on formally characterizing the semantics and complexity of RefL, and in [30], we focus on optimizations that are needed in practice.

## References

1. Dinesh, N., Joshi, A., Lee, I., Sokolsky, O.: Reasoning about conditions and exceptions to laws in regulatory conformance checking. In: Ninth Interntational Conference on Deontic Logic in Computer Science (DEON). (2008)
2. U.S. Food and Drug Administration: Code of Federal Regulations. http://www.gpoaccess.gov/cfr/index.html
3. Abrahams, A.: Developing and Executing Electronic Commerce Applications with Occurrences. PhD thesis, Univeristy of Cambridge (2002)
4. Breaux, T.D., Vail, M.W., Anton, A.I.: Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations. In: Proceedings of the 14th IEEE International Requirements Engineering Conference. (2006)
5. Giblin, C., Liu, A., Muller, S., Pfitzmann, B., Zhou, X.: Regulations Expressed as Logical Models (REALM). In Moens, M.F., Spyns, P., eds.: Legal Knowledge and Information Systems. (2005)
6. Ross, A.: Directives and Norms. Routlege and Kegan Paul (1968)
7. Boella, G., van der Torre, L.: Permissions and obligations in hierarchical normative systems. In: Proceedings of the 9th international conference on AI and law. (2003)

8. Reiter, R.: A logic for default reasoning. In: Readings in nonmonotonic reasoning. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA (1987) 68–93
9. McCarty, L.T.: A language for legal discourse - i. basic features. In: Proceedings of ICAIL. (1989)
10. Sergot, M., F.Sadri, Kowalski, R., F.Kriwaczek, P.Hammond, Cory, H.: The british nationality act as a logic program. Communications of the ACM **29**(5) (1986) 370–86
11. Kripke, S.: Outline of a theory of truth. Journal of Philosophy **72** (1975) 690–716
12. Dinesh, N., Joshi, A., Lee, I., Sokolsky, O.: Logic-based regulatory conformance checking. In: Proceedings of the 14th Monterey Workshop. (2007)
13. Bench-Capon, T., Robinson, G., Routen, T., Sergot, M.: Logic programming for large scale applications in law: A formalisation of supplementary benefit legislation. In: Proceedings of the 1st International Conference on AI and Law. (1987)
14. Holzmann, G.: The Spin model checker. IEEE Trans. on Software Engineering **23**(5) (1997) 279–295
15. Makinson, D., van der Torre, L.: Input/output logics. Journal of Philosophical Logic **29** (2000) 383–408
16. Makinson, D., van der Torre, L.: Permissions from an input/output perspective. Journal of Philosophical Logic **32**(4) (2003)
17. Prakken, H., Sergot, M.: Contrary-to-duty obligations. Studia Logica **57**(1) (1996) 91–115
18. Marcus, R.B.: Iterated deontic modalities. Mind **75**(300) (1966)
19. Sistla, A.P., Clarke, E.M.: The complexity of propositional linear temporal logic. ACM **32** (1985) 733–49
20. Rudin, W.: Real and Complex Analysis. McGraw-Hill Book Company (1987)
21. Chisholm, R.: Contrary-to-duty imperatives and deontic logic. Analysis **24** (1963)
22. Vardi, M.: The complexity of relational query languages. In: STOC. (1982)
23. Gradel, E., Otto, M., Rosen, E.: Undecidability results on two-variable logics. Archive for Mathematical Logic **38** (1999)
24. Lakemeyer, G., Levesque, H.: Towards an axiom system for default logic. In: Proceedings of the AAAI Conference. (2006)
25. Fitting, M.: Many-valued modal logics. Fundamenta Informaticae **15** (1991)
26. Halpern, J., Lakemeyer, G.: Multi-agent only knowing. Journal of Logic and Compuation **11**(1) (2001)
27. Lichtenstein, O., Pnueli, A.: Propositional temporal logics: Decidability and completeness. Logic Journal of the IGPL **8**(1) (2000)
28. Fitting, M.: A Kripke/Kleene Semantics for logic programs. Journal of Logic Programming **2** (1985)
29. Monteiro, L., Porto, A.: A language for contextual logic programming. In Apt, K., de Bakker, J., Rutten, J., eds.: Logic Programming Languages: Constraints, Functions, and Objects. (1993)
30. Dinesh, N., Joshi, A., Lee, I., Sokolsky, O.: Checking traces for regulatory conformance. In: Proceedings of the Workshop on Runtime Verification. (2008)